526935

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

Rec'd PCT/PTO 08 MAR 2005

(43) 国際公開日
2005年1月13日 (13.01.2005)

PCT

(10) 国際公開番号
WO 2005/004418 A1

(51) 国際特許分類[7]: H04L 12/56

(21) 国際出願番号: PCT/JP2004/009446

(22) 国際出願日: 2004年7月2日 (02.07.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-271202 2003年7月4日 (04.07.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町二丁目3番1号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 久田 裕介 (HISADA, Yusuke) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目9番11号NTT知的財産センタ内 Tokyo (JP). 鶴岡 行雄 (TSURUOKA, Yukio) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目9番11号NTT知的財産センタ内 Tokyo (JP). 小野 諭 (ONO, Satoshi) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目9番11号NTT知的財産センタ内 Tokyo (JP).

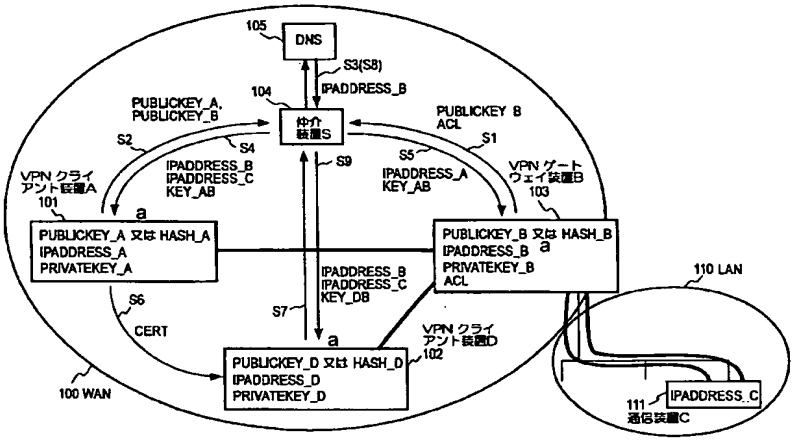
(74) 代理人: 草野 卓, 外 (KUSANO, Takashi et al.); 〒1600022 東京都新宿区新宿四丁目2番21号 相模ビル Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,

[続葉有]

(54) Title: REMOTE ACCESS VPN MEDIATION METHOD AND MEDIATION DEVICE

(54) 発明の名称: リモートアクセスVPN仲介方法及び仲介装置



101...VPN CLIENT DEVICE A
a...OR
104...MEDIATION DEVICE S
103...VPN GATEWAY DEVICE B
102...VPN CLIENT DEVICE D
111...COMMUNICATION DEVICE C

(57) Abstract: A mediation device is provided on an IP network for storing an access control list (ACL) stored in a VPN gateway device. The mediation device receives a search request from a VPN client device, references the ACL to acquire a private IP address of a communication device,

[続葉有]

WO 2005/004418 A1

LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

searches DNS to acquire an IP address of a VPN gateway device, generates a common key used for authentication and encrypted communication between the VPN client device and the VPN gateway device, transmits the IP address of the VPN gateway device, the private IP address of the communication device, and the common key to the VPN client device, and transmits the IP address of the VPN client device and the common key to the VPN gateway device.

(57) 要約: ＩＰネットワーク上に仲介装置を設け、VPNゲートウェイ装置で保管されるアクセスコントロールリスト(ACL)を記憶する。仲介装置は、VPNクライアント装置から検索要求を受信し、ＡＣＬを参照して通信装置のプライベートＩＰアドレスを取得し、DNSを検索してVPNゲートウェイ装置のＩＰアドレスを取得し、VPNクライアント装置とVPNゲートウェイ装置との間の認証と暗号化通信に用いる共通鍵を生成し、VPNゲートウェイ装置のＩＰアドレス、通信装置のプライベートＩＰアドレス及び共通鍵をVPNクライアント装置に送信し、VPNクライアント装置のＩＰアドレス及び共通鍵をVPNゲートウェイ装置に送信する。

明 細 書

リモートアクセスVPN仲介方法及び仲介装置

技術分野

[0001] 本発明は、インターネットにおいて、IPsec(IPsecurity Protocol)、L2TP(Layer2 Tunneling Protocol)等の任意のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いられる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNクライアント装置とVPNゲートウェイ装置の間で認証に用いる相互認証情報を、VPNクライアント装置とVPNゲートウェイ装置の間で安全に共有する技術に関する。

背景技術

[0002] インターネット上に構築される仮想の閉域ネットワークは一般にバーチャル プライベート ネットワーク(Virtual Private Network:以後VPNと略す)と呼ばれる。VPNはIPsec、L2TP等のトンネリングプロトコルを用いて構築され、ローカルエリアネットワーク(LAN)内のリソースに移動クライアントからインターネット経由でアクセスしたり、または、物理的に離れた複数のローカルエリアネットワークをインターネット経由で接続する場合に利用される。 リモートユーザにリモートアクセスVPNへのアクセスを許可する場合、アクセスするVPNクライアント、アクセスされるVPNゲートウェイの双方に以下のような設定が必要になる。

[0003] VPNクライアント装置では、

・VPNゲートウェイ装置(グローバル)IPアドレス

・VPNゲートウェイ装置とVPNクライアント装置との相互認証情報

・VPNクライアント装置のプライベートIPアドレス

・VPN内部ネットワークのルータ、ネームサーバ(DNS, WINSなど)のプライベートIPアドレス(VPNクライアント側で静的に設定する場合)

VPNゲートウェイ装置では、

・VPNゲートウェイ装置とVPNクライアント装置との相互認証情報

・認証したVPNクライアント装置に払い出すプライベートIPアドレス、VPN内部のル

ータ、ネームサーバのプライベートIPアドレス(VPNゲートウェイ側から動的に設定・通知する場合)

一般にこれらの設定はセキュリティに関わることから、安全確実に行う必要があり、VPNクライアントの利用者にも、VPN管理者にも多大な負担を与える。また、このVPNへアクセス可能なユーザの変化が激しい場合は、ユーザ管理に関わる負担も多大になる。さらに、ユーザが複数のVPNにアクセスする場合、接続対象VPNそれぞれに対し、認証方法や認証情報、それを保管するICカードなどの認証デバイスが異なる場合もあり、その管理が多大な負担になる。

[0004] VPNクライアント装置は、自分に許可されたVPNへのアクセス権限を一時的に他のVPNクライアント装置において実施したい場合がある。また、VPNクライアント装置(A)がNAT(ネットワークアドレス変換)セグメントの内側にあったり、電力制限の厳しい携帯小型デバイスなどの場合、VPNゲートウェイ装置との暗号化通信路を直接確立するのは適当とはいえない。この場合、典型的には、当該NATセグメントとインターネットとのゲートウェイ機能をもつ別のVPNクライアント装置(D) がVPNゲートウェイとのトンネル確立を受け持つことになる。この場合、アクセス制御は、VPNクライアント装置(D)に対して行うのではなく、VPNクライアント装置(A)に対して行うことが必要になる。このように、アクセス権限が許可されているVPNクライアント装置とトンネルの始点となるVPNクライアント装置とが異なる場合には、権限を委譲する機構が不可欠になる。

[0005] さらに、VPNの提供するサービスの性質によっては、VPNクライアントのユーザは、VPNサービスを行っている側に対し、厳密に個人を特定できる情報を知られたくない場合も存在する。一方、VPNサービスを提供する側も、クライアント認証情報などの個人情報の取り扱いや、会員加入脱退管理などの煩雑な業務はアウトソーシングして本来のサービス提供に専念したい場合も多い。この場合、ユーザ認証やアクセス権限の検証はアウトソーサに実行させ、正当な利用者のみをVPNサービス提供者に仲介してもらうことになる。

共通鍵を安全に配布する方法としては種々の方法がある(例えば、特許文献1、特許文献2参照)。特許文献1に示される方法は、ローカルエリアネットワークに接続された複数の通信装置との間で共通鍵を交換する方法で、DHCPサーバ機能を有する

ゲートウェイ装置を介して共通鍵を交換する。具体的には、ローカルエリアネットワークへの接続時にDHCPに従いIPアドレスを取得する際に、共通鍵も同時に交換する。これによって、ローカルエリアネットワーク内の通信を暗号化するための共通鍵を交換できる。

[0006] 特許文献2に示される方法は、インターネットに接続されたVPNクライアント装置と、VPNゲートウェイ装置で管理されるローカルエリアに接続された通信装置との通信において、VPNクライアント装置とVPNゲートウェイ装置との間である共通鍵を交換し、VPNゲートウェイ装置と通信装置との間で別の共通鍵を交換する方法である。これによって、VPNクライアント装置とローカルエリアネットワークに接続された通信装置との間でIKE等の鍵交換方式を用いて鍵交換を行う必要なく、VPNクライアント装置とローカルエリアネットワークに接続された通信装置との暗号通信を実現できる。

[0007] しかし、特許文献1の方法は、鍵配布が可能な範囲はローカルエリアネットワークに限られ、また、特許文献2の方法は、前もってVPNクライアント装置とVPNゲートウェイ装置との間である共通鍵を交換する必要があることから、会員の加入・脱退が頻繁におきる場合の管理業務が煩雑になる。また、いずれの方法も、アクセス制御を第三者に仲介させたり、VPNクライアント装置が、接続を許可されたVPNゲートウェイ装置へのアクセスについて、暗号化通信の処理を他の信頼できるVPNクライアント装置に委譲する機能はない。 認証したVPNクライアント装置に払い出すプライベートIPアドレス、VPN内部のルータ、ネームサーバのプライベートIPアドレスなどの構成管理情報をVPNゲートウェイ側から動的に設定・通知する方法として、種々の方法がある。(例えば、特許文献3、特許文献4、非特許文献1、非特許文献2、非特許文献3参照)

特許文献3に示される方法では、設定情報を管理する管理装置を儲け、管理情報が通信装置に設定情報を転送する際に、通信装置のIPアドレスとログインパスワードを提示してその通信装置にログインし、設定情報を転送する方法を示している。これによれば、VPNゲートウェイ装置に相当する管理装置から設定情報としてプライベートIPアドレス等の構成管理情報をVPNクライアント装置に配布できる。しかしながら、この方法は、受信者であるVPNクライアント装置の認証を行っておらず、IPアドレスの偽装による成りすまし攻撃、中間者攻撃にさらされる危険がある。また、VPNクライアント

装置から構成管理情報取得の要求が出される場合、管理装置がどのようにして認証・アクセス制御を行うのか示されていない。

[0008] 特許文献4、非特許文献1、非特許文献2、非特許文献3 は、いずれもIPsec や PPP、L2TPなどのトンネリングプロトコルで構成管理情報を動的に設定・通知する方法を示している。

本発明も、VPNクライアント装置とVPNゲートウェイ装置間での各種トンネルプロトコルのセットアップフェーズにおいて、上記動的設定・通知に対応した機能が実施されることを仮定している。ただし、従来の方式がトンネルのセットアップ時にユーザ認証やアクセス制御と上記構成管理情報の動的設定・通知を一体として扱っているのに対し、本発明は、ユーザ認証とアクセス制御は仲介装置にて実施し、VPNクライアント装置とVPNゲートウェイ装置が共通の秘密を共有できるようにし、それに基づいてVPNクライアント装置とVPNゲートウェイ装置との間のトンネルセットアップが行われ、その後、トンネルの構成管理情報がVPNゲートウェイ装置から動的に設定・通知される点が異なる。また、VPNクライアント装置Bが、暗号化通信などのトンネルプロトコル処理を他の信頼できるVPNクライアント装置Dに委譲することにより、仲介装置におけるアクセス権限の検査は要求元装置Bに対しておこなわれるようにできる。ただし、管理上の都合によっては、トンネルの構成管理情報の一部、当該トンネルへのルーティング情報などネットワークの運用に関する情報を仲介装置からVPNクライアント装置に送信してもよい。この場合、情報の種類に応じて、トンネルのセットアップの開始前あるいは完了後に仲介装置から送られてきた構成管理情報等を設定する。

また、公開鍵を用いた認証方法、証明書発行方法としてSPKI(Simple Public Key Infrastructure)方式がある(例えば、非特許文献4、非特許文献5)が、リモートアクセスVPNへの利用方法について明らかでない。

特許文献1:特開2001-292135号公報

特許文献2:特開2002-271309号公報

特許文献3:特開 2003-18163号公報

特許文献4:特開2001-160828号公報

非特許文献1:B.Patel,B.Aboba,S.Kelly,V.Gupta,"Dynamic Host Configuration

Protocol(DHCPv4) Configuration of IPsec Tunnel Mode", [online]、2003年1月掲載、RFC3456、Internet Engineering Task Force、[2003年3月17日検索]、インターネット<URL:http://www.ietf.org/rfc/rfc3456.txt>

非特許文献2:IPCP (RFC-1332)

非特許文献3:EAP (RFC-2284)

非特許文献4:C.Ellison, B.Frantz, B.Lampson, R.Rivest, B.Thomas, T.Ylonen, "SPKI Certificate Theory", [online]、1999年9月掲載、RFC2693、Internet Engineering Task Force、インターネット<URL:http://www.ietf.org/rfc/rfc2693.txt>

非特許文献5:C.Ellison, B.Frantz, B.Lampson, R.Rivest, B.Thomas, T.Ylonen, "Simple Public Key Infrastructure <draft-ietf-spki-cert-structure-06.txt>", [online]、1999年7月26日掲載、Internet Engineering Task Force、インターネット<URL:http://world.std.com/~cme/spki.txt>

発明の開示

発明が解決しようとする課題

[0009] 本発明は上述のような課題に鑑みなされたものであり、IPネットワークにおいて、IPsec、L2TP等の任意のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNゲートウェイ装置により管理されるローカルエリアネットワーク内の任意の通信装置のプライベートIPアドレス、及び、VPNクライアント装置とVPNゲートウェイ装置の間でIKE(Internet Key Exchange)フェーズ1における認証に用いる共通鍵を、VPNクライアント装置とVPNゲートウェイ装置との間で安全に共有できるようにすることである。また、リモートアクセスVPNにおける認証において、利用者の個人情報を通信する相手に知られずに通信できるようにすることである。

課題を解決するための手段

[0010] この発明によれば、IPネットワークにバーチャルプライベートネットワーク、以下VPN、クライアント装置及びVPNゲートウェイ装置が接続され、VPNゲートウェイ装置により管理されるローカルエリアネットワークに通信装置が接続され、前記IPネットワークに接続された任意のVPNクライアント装置と、VPNゲートウェイ装置、及び、VPNゲートウ

ェイ装置に管理されるローカルエリアネットワークに接続された任意の通信装置との間のトンネリングプロトコルによるリモートアクセスVPNを実行するシステムにおけるリモートアクセスVPN仲介方法であり、

(a) 前記IPネットワーク上に設けられた仲介装置に、前記VPNゲートウェイ装置から前記通信装置に割り当てられたプライベートIPアドレスを示す情報を含むアクセスコントロールリストを送信する過程と、

(b) 前記仲介装置で前記アクセスコントロールリストを前記VPNゲートウェイ装置に対応して記憶する過程と、

(c) 前記VPNクライアント装置からの要求に応答して前記VPNゲートウェイ装置に対応するIPアドレスを検索し、上記アクセスコントロールリストから対応する前記通信装置のプライベートIPアドレスを取得し、前記VPNクライアント装置に送ると共に、前記クライアント装置のIPアドレスを前記VPNゲートウェイ装置に送り、前記VPNクライアント装置と前記ゲートウェイ装置との間の認証された暗号化トンネルをセットアップするために用いる相互認証情報を生成し、前記VPNクライアント装置と前記ゲートウェイ装置の双方に送る過程と、

(d) 前記相互認証情報を用いて前記VPNクライアント装置と前記ゲートウェイ装置間で認証された暗号化トンネルセットアップを行い、この暗号化トンネルを通して前記通信装置のプライベートIPアドレスを使ってリモートアクセスを実行する過程、

とを含む。

[0011] この発明によれば、IPネットワークにVPNクライアント装置及びVPNゲートウェイ装置が接続され、VPNゲートウェイ装置により管理されるローカルエリアネットワークに通信装置が接続され、前記IPネットワークに接続された任意のVPNクライアント装置と、VPNゲートウェイ装置、及び、VPNゲートウェイ装置に管理されるローカルエリアネットワークに接続された任意の通信装置との間のトンネリングプロトコルによるリモートアクセスVPNを実行するシステムにおいて、IPネットワーク上に設置されて、リモートアクセスVPNの確立を仲介する仲介装置であって、

前記VPNゲートウェイ装置から送信される前記通信装置に割り当てられたプライベートIPアドレスを示す情報を含むアクセスコントロールリスト、以下ACL、を記憶する

ACL記憶手段と、

前記VPNクライアント装置、前記ゲートウェイ装置を認証し、アクセス権限制御を実行する認証／アクセス権限制御手段と、

前記アクセスコントロールリストを参照して、前記通信装置に割り当てられたプライベートIPアドレスを取得し、ドメインネームサーバを検索して前記VPNゲートウェイ装置に割り当てられたIPアドレスを取得するIPアドレス取得手段と、

前記VPNクライアント装置と前記VPNゲートウェイ装置との間の認証された暗号化トンネルをセットアップするために用いる相互認証情報を生成する認証情報生成手段と、

前記VPNクライアント装置に、前記VPNゲートウェイ装置のIPアドレス、前記通信装置のプライベートIPアドレス及び前記相互認証情報を送信し、前記VPNゲートウェイ装置に、前記VPNクライアント装置のIPアドレス及び前記相互認証情報を送信する通信手段、

とを含む。

発明の効果

[0012] 本発明においては、次のような効果を奏する。第1の効果は、IPネットワークにおいて、L2TP、IPsec等のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNゲートウェイ装置により管理されるローカルエリアネットワーク内の任意の通信装置のプライベートIPアドレス、及び、VPNクライアント装置とVPNゲートウェイ装置の間で暗号化されたトンネルをセットアップする際に相互認証に必要となる共通鍵ないし共通の秘密(以下、相互認証情報)を、VPNクライアント装置とVPNゲートウェイ装置との間で安全に共有できることである。その理由は、仲介装置においてプライベートIPアドレスを安全に管理し、プライベートIPアドレスと相互認証情報を安全に配布するためである。

[0013] 具体的には、プライベートIPアドレスの仲介装置への登録において、VPNゲートウェイ装置を認証し、認証に成功した場合に限り、通信路を暗号化し、暗号化した通信路を用いて、プライベートIPアドレスを受信する。また、プライベートIPアドレスの検索に

おいて、VPNクライアント装置を認証し、認証に成功した場合に限り、VPNクライアント装置の公開鍵を用いてアクセス権限制御を実行し、アクセス権限制御に成功した場合に限り、VPNゲートウェイ装置のグローバルIPアドレスをドメインネームサーバDNSから取得し、仲介装置とVPNクライアント装置との間の通信路を暗号化し、暗号化した通信路を用いて、VPNゲートウェイ装置のグローバルIPアドレスと、通信装置のプライベートIPアドレスと、相互認証情報をVPNクライアント装置に送信し、また、仲介装置とVPNゲートウェイ装置との通信路を暗号化し、暗号化した通信路を用いて、VPNクライアント装置のグローバルIPアドレスと、相互認証情報及びVPNクライアント装置の属性情報をVPNゲートウェイ装置に送信するためである。

[0014] 第2の効果は、リモートアクセスVPNにおける認証において、利用者の個人情報を通信する相手に知られずに通信できる手段を提供することである。その理由は、PKI方式に従って認証する場合には、個人情報を含む公開鍵証明書を通信相手に送信する代わりに仲介装置に送信して認証するためである。また、SPKI方式に従って認証する場合には、いかなる証明書も個人情報を含まないように証明書の形式を定義できるためである。一方、仲介装置は、認証結果に伴う属性情報をVPNゲートウェイ装置に送信することができ、当該VPNクライアント装置を収容するVLAN を選択する機能、当該VPNゲートウェイ装置のパケットフィルタリング設定を変更する機能、VPN内の内部向けDNSの逆引き辞書において、VPNクライアント装置のプライベートIPアドレスに対応したエントリに当該属性情報を追加する機能などと連携させてもよい。

図面の簡単な説明

[0015] [図1]本発明の第1の実施例におけるシステム構成例を示す図である。

[図2]本発明の第1の実施例の動作概要を説明する図である。

[図3]この発明の仲介装置(S)104の機能構成を示す図である。

[図4]AはACLとハッシュ値を対応させた表を示す図、Bは図4A中のACLエントリの1つの例を示す図である。

[図5]本発明の第1の実施例におけるアクセスコントロールACLの記憶手段を示す図である。

[図6]本発明の第1の実施形態におけるIPアドレス及び共通鍵の送信手順を示す図

である。

[図7]本発明の第1の実施例における仲介装置でのIPアドレスの取得手順、及び、共通鍵の生成手順の詳細処理フロー図である。

[図8]本発明の第1の実施例におけるアクセスコントロールリストACLの一例である。

[図9]本発明の第1の実施例におけるデータTAGの一例である。

[図10]本発明の第1の実施例における演算結果データDATAの一例である。

[図11]本発明の第1の実施例における証明書CERTの一例である。ネットワークを通してそのプログラムを配布したりすることが可能である。

[図12]本発明の第2の実施例におけるシステム構成例を示す図である。

[図13]本発明の第2の実施例の動作概要を説明する図である。

[図14]本発明の第2の実施例におけるアクセスコントロールACLの記憶手段を示す図である。

[図15]本発明の第2の実施例における仲介装置でのアクセスコントロールリストACLの記憶手順の詳細処理フロー図である。

[図16]本発明の第2の実施例におけるIPアドレス及び共通鍵の配布手順を示す図である。

[図17]本発明の第2の実施例における、仲介装置でのIPアドレスの取得手順、及び、共通鍵の生成手順の詳細処理フロー図である。

[図18]本発明の第3の実施例におけるVPNクライアント装置の実施例を示す図。

[図19]本発明の第4の実施例におけるVPNゲートウェイ装置が使用されるネットワーク全体の構成を示す図。

[図20]第4の実施例で使用されるアクセスコントロールリストの例を示す図。

[図21]第4の実施例で使用されるVPNゲートウェイ装置の機能構成例を示す図。

発明を実施するための最良の形態

[0016] 以下に、本発明の実施の形態について図面を参照して詳細に説明する。

実施例1

これは、SPKI(Simple Public Key Infrastructure)方式に従って、仲介装置がVPNクライアント装置やVPNゲートウェイ装置を認証し、また、VPNクライアント装置が権限委

譲の証明書を発行する実施例である。このSPKI方式では認証局は不要である。

図1に本実施例の全体的システム構成を示す。図1において、VPNクライアント装置(A)101、VPNクライアント装置(D)102、VPNゲートウェイ装置(B)103、仲介装置(S)104、ドメインネームサーバ(DNS)105はそれぞれIP(Internet Protocol)に従って広域ネットワーク(Wide Area Network:WAN)100に接続されている。また。通信装置(C)111が、VPNゲートウェイ装置(B)103をゲートウェイ装置とするローカルエリアネットワーク(LAN)110に接続されている。また、VPNゲートウェイ装置(B)103に対するアクセスコントロールリストを管理する権限を有するVPNゲートウェイ管理装置(M)112を更にWAN上に設けても良い。

[0017] 図2は、図1の全体の動作を説明するための図である。太線はIPsecトンネルモードによるVPNを示している。

ここで、VPNクライアント装置(A)101のホスト名は公開鍵PUBLICKEY_A(またはそのハッシュ値HASH_A)、IPアドレスはIPADDRESS_Aとする。VPNクライアント装置(D)102のホスト名は公開鍵PUBLICKEY_D(またはそのハッシュ値HASH_D)、IPアドレスはIPADDRESS_Dとする。また、VPNゲートウェイ装置(B)103のホスト名は公開鍵PUBLICKEY_B(またはそのハッシュ値HASH_B)、IPアドレスはIPADDRESS_Bとする。すなわち、VPNクライアント装置やVPNゲートウェイ装置は、それぞれ、その公開鍵(またはそのハッシュ値)で識別可能である。通信装置(C)111のプライベートIPアドレスはIPADDRESS_Cとする。

[0018] VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、及び、VPNクライアント装置(D)102に割り当てられたIPアドレスIPADDRESS_Dはいずれもネットワーク(WAN)100において一意であり、任意の手段で動的に割り当てられる。VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY_BとIPアドレスIPADDRESS_Bはドメインネームサーバ(DNS)105において一意に関連付けられて管理される。また、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cはローカルエリアネットワーク(LAN)110において一意であり、任意の手段を用いて動的に割り当てられる。

[0019] VPNクライアント装置(A)101、VPNクライアント装置(D)102、VPNゲートウェイ装置

(B)103、及び、仲介装置(S)104は、IPsecトランスポートモード、または、IPsecトンネルモードにより通信路を暗号化する手段を有する。また、VPNクライアント装置(A)101は、公開鍵PUBLICKEY_Aと対の秘密鍵PRIVATEKEY_Aを、PUBLICKEY_Aとともに保管している。VPNゲートウェイ装置(B)103は、公開鍵PUBLICKEY_Bと対の秘密鍵PRIVATEKEY_Bを、PUBLICKEY_Bとともに保管している。VPNクライアント装置(D)102は、公開鍵PRIVATEKEY_Dとの対の秘密鍵PRIVATEKEY_DをPUBLICKEY_Dとも保管している。VPNゲートウェイ装置(B)103は、ローカルエリアネットワーク110上の通信装置111に対するアクセスに要求される条件を記述したアクセスコントロールリスト(ACL)を保管している。

[0020] 図8に本実施例におけるアクセスコントロールリスト(ACL)の例を示す。アクセスコントロールリスト(ACL)の文法はSPKIに関する先の非特許文献4及び非特許文献5で定義されている。図8の例では、アクセス主体は、サブジェクトフィールド(subject)に書き込まれているハッシュsha1による公開鍵のハッシュ値がHASH_Aを有していることが指定され、タグフィールド(tag)に記載されたsha1ハッシュ値HASH_Bを有するVPNゲートウェイ装置103に接続されたローカルエリアネットワーク110上のプライベートIPアドレスIPADDRESS_Cを有する通信装置111へのアクセスが可能であることを示している。属性情報"ATTRIBUTE_A"のフィールドは、付加的機能として設けられ、例えば「無料ユーザ」と「有料ユーザ」で割り当てるプライベートアドレス範囲を変えて、VPNゲートウェイ装置(B)103においてパケットフィルタリングによりアクセスできるサーバを変化させたり、Webサーバがクライアントに提供するサービスをソースアドレスに基づいて変更できるようにする。"validity"のフィールドは、ACLのこのエントリーが有効な期間を示している。"propagate"はアクセス主体の権限委譲許可を示すが、本実施例では権限委譲がなされていないため、他のフィールドと共に認証のための単なるデータ値として使用される。

[0021] 仲介装置(S)104は、図3に示すように、アクセスコントロールリスト(ACL)記憶手段1041と、認証／アクセス権限制御手段1042と、IPアドレス取得手段1043と、相互認証情報生成手段としての鍵生成手段1044と、暗号化手段1045eを有する通信手段1045と、これらの動作を制御する動作制御手段1046とから構成されている。IPアドレス取

得手段1043は、VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY_Bをドメインネームサーバ(DNS)105に提示して、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを取得する。ACL記憶手段1041は、VPNゲートウェイ装置(B)103から登録されたアクセスコントロールリスト(ACL)を表として記憶する。認証／アクセス権限制御手段1042は、SPKI方式に基づいて、VPNクライアント装置(A)101、VPNゲートウェイ装置(B)103を認証し、及び／または、アクセス権限制御を実行する。通信手段1045は暗号化手段1045eを有しており、通信路を暗号化して、情報を安全に送受信する。相互認証情報生成手段としての鍵生成手段1044は、後述の相互認証情報としての共通鍵KEY_AB、及び、KEY_DBを生成する。

[0022] 上記IPアドレス取得手段1043では、DNS方式と呼ばれるインターネットにおける一般的なIPアドレス検索方式(名前解決方式)に従って、公開鍵PUBLICKEY_BからIPアドレスIPADDRESS_Bを検索する。また、上記ACL記憶手段1041では、公開鍵PUBLICKEY_Bとアクセスコントロールリスト(ACL)を例えば図4Aに示すようにACLテーブル1041Tとして関連付けて管理する。図1にはVPNゲートウェイ装置を1つしか示していないが、実際には複数のVPNゲートウェイ装置がそれぞれのローカルエリアネットワークをWAN100に接続しており、また、各ローカルエリアネットワーク上には、図1では1つしか示してないが、複数の通信装置が接続されているものとする。図4Aでは、それぞれのVPNゲートウェイ装置の公開鍵のハッシュ値と対応してアクセスコントロールリストが登録されている。

[0023] ACLテーブル1041T中の各アクセスコントロールリストACL、例えばACL1、は図4Bに表ACL1として示すように、帰属するローカルエリアネットワーク上のそれぞれの通信装置のプライベートIPアドレスに対応して、それらにアクセスする主体(subject)、例えばVPNクライアント装置が固有に有している公開鍵のハッシュ値を示してある。図4Bの表中の1行目の例では、プライベートIPアドレスIPADDRESS_C1の通信装置に対して、ハッシュ値HASH_Aを有するVPNクライアント装置にアクセスを許可することを示している。具体的には前述の図8に示す形態で記述される。各アクセス対象装置に対して設けられるアクセスコントロールリストACL中のアクセス主体は、図4A及び図8例のような公開鍵のハッシュ値だけでなく、例えば、ある会社の社員であることを証明

する社員番号、あるグループの会員であることを証明する会員番号、ある資格を有していることを証明する番号、など、様々なものが可能である。

[0024] 上記認証／アクセス権限制御1042では、SPKI方式に従い、VPNクライアント装置(A)101、VPNゲートウェイ装置(B)103、及び、VPNクライアント装置(D)102を認証する。具体的には、VPNクライアント(A)の秘密鍵PRIVATEKEY_Aによる署名SIG_Aと公開鍵PUBLICKEY_Aが入力されると、その公開鍵を使って署名SIG_Aを確認することにより、その公開鍵PUBLICKEY_Aに対応する秘密鍵PRIVATEKEY_Aを有するVPNクライアント(A)の本人性を証明する。また、秘密鍵PRIVATEKEY_Bによる署名SIG_Bと公開鍵PUBLICKEY_Bをすべて入力して、署名SIG_Bを確認することにより、秘密鍵PRIVATEKEY_Bを有するVPNゲートウェイ装置(B)の本人性を証明する。同様に、秘密鍵PRIVATEKEY_Dによる署名SIG_D、及び、公開鍵PUBLICKEY_Dを入力して、署名SIG_Dを確認することにより、秘密鍵PRIVATEKEY_Dを有するVPNクライアント(D)の本人性を証明する。

[0025] また、上記認証／アクセス権限制御1042では、SPKI方式に従い、VPNゲートウェイ装置(B)103に対するVPNクライアント装置(A)101及びVPNクライアント装置(D)102のアクセス権限を制御する。VPNゲートウェイ装置(B)103に対するVPNクライアント装置(A)101のアクセス権限を制御する場合には、VPNゲートウェイ装置(B)103のIPアドレスIPADDRESS_Bを検索するためのDNSクエリQUERY、署名SIG_A、及びアクセスコントロールリスト(ACL)を入力して、これらをデータ値として使用してSPKIに関する非特許文献4、及び、非特許文献5において定義される5-tuple reduction演算規則、及び／または、4-tuple reduction演算規則に基づく演算を実行して、演算結果を出力する。また、VPNゲートウェイ装置(B)103に対するVPNクライアント装置(D)102のアクセス権限を制御する場合には、VPNゲートウェイ装置(B)103のIPアドレスIPADDRESS_Bを検索するためのDNSクエリQUERY、署名SIG_D、SPKIに関する非特許文献4及び非特許文献5において定義される証明書CERT、及び、アクセスコントロールリスト(ACL)を入力して、SPKIに関する非特許文献4、及び、非特許文献5において定義される5-tuple reduction演算規則、及び／または、4-tuple reduction演算規則に基づく演算を実行して、演算結果を出力する。演算結果の具体例については、

図10を参照して後述する。

[0026] また、上記鍵生成手段1044は、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103との間のIKEフェーズ1における認証に用いる共通鍵KEY_AB、または、VPNクライアント装置(D)102とVPNゲートウェイ装置(B)103との間のIKEフェーズ1における認証に用いるKEY_DBをそれぞれ生成する。

また、VPNクライアント装置(A)101は、SPKI方式に従って、VPNクライアント装置(D)102に対し権限委譲の証明書CERTを発行する機能を有する。SPKIに関する非特許文献4及び非特許文献5においては、権限証明書(Authorization Certificate)と名前証明書(Name Certificate)の2種類の証明書について、それぞれ文法を定義している。本実施例においては、説明を簡単にするために、証明書CERTは権限証明書の1種類であると定義する。

[0027] 図11に本実施例における証明書CERTの具体例を示す。SPKIに関する非特許文献4及び非特許文献5によれば、権限証明書は、発行者の秘密鍵と一意に対応した公開鍵またはその公開鍵のハッシュ値を定義するissuerフィールド、権限の行使者、即ちここではVPNクライアント(D)、の秘密鍵と一意に対応した公開鍵またはその公開鍵のハッシュ値を定義するsubjectフィールド、権限内容を定義した文字列を含むtagフィールド、権限委譲を許可するか否かを定義した文字列を含むdelegationフィールド、及び、権限証明書の有効期間を定義した文字列を含むvalidityフィールドから構成されるデータ(以後、本データを証明書情報INFOと呼ぶ)に対し、発行者の秘密鍵で署名したデータである。

[0028] この定義に基づき、本実施例における証明書CERTの証明書情報INFOにおけるissuerフィールドの値は、証明書情報INFOの発行者の公開鍵PUBLICKEY_Aまたは任意のハッシュ演算アルゴリズムによる公開鍵PUBLICKEY_Aのハッシュ値HASH_Aであると定義する。subjectフィールドの値は、権限を受ける者の公開鍵PUBLICKEY_Dまたは任意のハッシュ演算アルゴリズムによる公開鍵PUBLICKEY_Dのハッシュ値HASH_Dであると定義する。tagフィールドの値は、VPNゲートウェイ装置(B)103のIPアドレスIPADDRESS_Bを検索するためのDNS クエリを許可するためのデータであり、その中には、VPNゲートウェイ装置(B)103の公開鍵 PUBLICKEY_B また

は任意のハッシュ演算アルゴリズムによる公開鍵 PUBLICKEY_B のハッシュ値 HASH_B を含むとする。delegationフィールドの値は、非特許文献4において定義される文字列"propagate"であると定義する。一方、validityフィールドの値は、本発明とは直接関係しないため、いかなる値も定義しないものとする。また、証明書情報INFOに秘密鍵PRIVATEKEY_Aを用いて署名する。

[0029] 次に、図2を参照して、図1の動作概要を説明する。アクセスコントロール(ACL)の登録(記憶)時、VPNゲートウェイ装置(B)103は、公開鍵PUBLICKEY_B(またはそのHASH_B)とアクセスコントロール(ACL)を仲介装置(S)104に送信する(ステップS1)。仲介装置(S)104は該公開鍵PUBLICKEY_B(またはそのHASH_B)とアクセスコントロール(ACL)を記憶する。

VPNゲートウェイ装置(B)103を経由して、VPNクライアント装置(A)101から通信装置(C)111にIPsecトンネルモードによるリモートVPNを実行する場合、VPNクライアント装置(A)101は、公開鍵PUBLICKEY_Aと公開鍵PUBLICKEY_B(又はそのHASH_AとHASH_B)を仲介装置(S)104に送信して、VPNゲートウェイ装置(B)103及び通信装置(C)IPアドレスの検索要求を行なう(ステップS2)。

[0030] 仲介装置(S)104は、SPKI方式に従ってVPNクライアント装置(A)101のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ(DNS)105を検索してVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを取得する(ステップS3)。また、仲介(S)104は、アクセスコントロール(ACL)を参照して、VPNゲートウェイ装置(B)103により管理されるLAN110に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを取得する。さらに、仲介装置(S)104は、VPNクライアント装置(A)101との間の認証に用いる共通鍵KEY_ABを生成する。そして、仲介装置(S)104は、VPNクライアント装置(A)101の公開鍵PUBLICKKEY_Aを使って仲介装置(S)104とVPNクライアント装置(A)101との間の通信路を暗号化し、VPNクライアント装置(A)101へIPADDRESS_B、IPADDRESS_C及び共通鍵KEY_ABを送信する(ステップS4)。また、仲介装置(S)104は、VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY_Bを使って仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信路を暗号化し、VPNゲートウェイ装置(B)103へ

IPADDRESS_AとKEY_ABを送信する(ステップS5)。これにより、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103間は共通鍵KEY_ABを使って安全に通信可能となる。なお、本実施例では、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103間のトンネリングプロトコルとしてIPsecトンネルモードを、また、両者が相互に認証するために仲介装置(S)104から送信する情報として、共通鍵を用いた。この他、トンネリングプロトコルとしてL2TP、PPTPなど別のプロトコルを用いたり、相互認証情報として、ID、パスワード、共通の秘密、SPKIの権限証明書など他の手段の情報を送信し、利用してもよい。

[0031] VPNクライアント装置(A)101がVPNゲートウェイ装置(B)103のIPアドレスを検索する権限をVPNクライアント装置(D)102委譲する場合は、VPNクライアント装置(D)102に対してSPKI方式に従って証明書CERTを送信する(ステップS6)。VPNクライアント装置(D)102は、公開鍵PUBLICKEY_DとCERT、及び公開鍵PUBLICKEY_B(またはそのHASH_B)を仲介装置(S)104に送信して、VPNゲートウェイ装置(B)103及び通信装置(C)のIPアドレスの検索要求を行なう(ステップS7)。

仲介装置(S)104は、SPKI方式に従ってVPNクライアント装置(D)102のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ(DNS)105を検索してVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを取得する(ステップS8)。また、仲介装置(S)104は、アクセスコントロール(ACL)を参照して、VPNゲートウェイ装置(B)103により管理されるLAN110に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを取得する。さらに、仲介装置(S)104は、VPNクライアント装置(D)102との間の認証に用いる共通鍵KEY_DBを生成する。そして、仲介装置(S)104は、VPNクライアント装置(D)102の公開鍵PUBLICKEY_Dを使って仲介装置(S)104とVPNクライアント装置(D)102との間の通信路を暗号化し、VPNクライアント装置(D)102へIPADDRESS_B、IPADDRESS_C及び共通鍵KEY_DBを送信する(ステップS9)。また、仲介装置(S)104は、VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY_Bを使って仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信路を暗号化し、VPNゲートウェイ装置(B)103へIPADDRESS_DとKEY_DBを送信する(ステップ10)。これにより、VPNクライアント装置

(D)102とVPNゲートウェイ装置(B)間は共通鍵KEY_DBを使って安全に通信可能となる。

[0032] 以上、図1に示すシステムの各装置の構成及び全体の動作概要を述べたが、ドメインネームサーバ(DNS)105におけるIPアドレスの管理及び名前解決方法、IPsecトランスポートモードまたはトンネルモードによる通信路の暗号化方法、共通鍵KEY_AB及びKEY_DBの生成方法、及び、公開鍵を用いた署名確認方法については、当業者にとってよく知られているので、その詳細な構成は省略する。また、SPKI方式におけるアクセス権限制御において、権限証明書に加え、名前証明書を用いる場合も本実施例と同様の方法で実施できるため、その詳細な説明については省略する。

[0033] 以下に、本実施例1におけるアクセスコントロールリスト(ACL)の記憶手順、及びIPアドレスの取得、共通鍵の生成、これらIPアドレスと共通鍵の送信手順について詳述する。 まず、図5を参照して、アクセスコントロールリスト(ACL) を仲介装置(S) に記憶する手順について説明する。なお、本実施例では、アクセスコントロールリストがVPNゲートウェイ装置(B)103自身に保管・管理されていることを仮定する。

VPNゲートウェイ装置(B)103と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1001)。これでVPNゲートウェイ装置(B)103と仲介装置(S)104との間の通信路が暗号化される。VPNゲートウェイ装置(B)103は、暗号化された通信路を用いて、公開鍵PUBLICKEY_BとSKPI形式のアクセスコントロールリスト(ACL)(図8)を送信する(ステップ1002)。仲介装置(S)104は、VPNゲートトウェイ装置(B)103から送信された公開鍵PUBLICKEY_Bとアクセスコントロールリスト(ACL)を受信して、該受信した公開鍵PUBLICKEY_Bとアクセスコントロールリスト(ACL)を関連づけて記憶する(ステップ1003)。VPNゲートウェイ装置(B)103と仲介装置(S)104は、接続を切断する(ステップ1004)。

[0034] なお、前述のVPNゲートウェイ装置(B)103に対するアクセスコントロールリスト(ACL)を管理する権限を有するVPNゲートウェイ管理装置(M)112を設けた場合は、図5に示したアクセスコントロールリスト(ACL)の登録手順において、VPNゲートウェイ装置(B)103による処理は全て、VPNゲートウェイ管理装置(M)112により実行される。

次に、図6及び図7を参照して、仲介装置(S)104が、VPNクライアント装置(A)101と

VPNゲートウェイ装置(B)103との間の共通鍵KEY_ABを生成し、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)に割り当てられたプライベートIPアドレスIPADDRESS_C、及び共通鍵KEY_ABをVPNクライアント装置(A)101に送信し、また、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、VPNクライアント装置の属性情報ATTRIBUTE_A及び、共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信する手順について説明する。

[0035] 図6において、VPNクラアント装置(A)101と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1101)。すなわち、VPNクライアント装置(A)101と仲介装置(S)104との間の通信路が暗号化される。VPNクライアント装置(A)101は、暗号化された通信路を用いて、VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY_Bを含むDNSクエリQUERY、及び、VPNクライアント装置(A)101の公開鍵PUBLICKEY_Aを送信する(ステップ1102)。

仲介装置(S)104は、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、VPNゲートウェイ装置(B)103により管理されるLAN110に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C及びVPNクライアント装置(A)101の属性情報ATTRIBUTE_Aを取得し、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103との間のIKE等の認証に用いる共通鍵KEY_ABを生成する(ステップ1103)。図7はステップ1103の詳細処理フローである。

[0036] 図7において、仲介装置(S)104は、VPNクライアント装置(A)101から送信されたDNSクエリQUERYと公開鍵PUBLICKEY_Aを受信して入力する(ステップ1201)。次に、入力したDNSクエリQUERYを参照して公開鍵PUBLICKEY_Bを取り出す(ステップ1202)。次に、取り出した公開鍵PUBLICKEY_Bをもとに、関連付けられたアクセスコントロールリスト(ACL)を取得する(ステップ1203)。アクセスコントロールリスト(ACL)は図8に示す形式をとる。次に、ステップ1201において入力したDNSクエリQUERYを用いて、図9に示す形式のデータTAGを生成する(ステップ1204)。

[0037] 仲介装置(S)104は、上記ステップ1201において入力した公開鍵PUBLICKEY_Aとステップ1204において生成したデータTAGとステップ1203において取得したアクセ

スコントロールリスト(ACL)を入力し、例えば、非特許文献4、及び、非特許文献5 において定義される演算規則に従って演算を実行し(ステップ1205)、演算に成功する否か判定する(ステップ1206)。演算に失敗した場合、この時点で処理を終了とする。

仲介装置(S)104は、ステップ1206において、演算に成功した場合と判定された場合に限り、図10に示す形式の演算結果のデータDATAを出力する。図10に示す演算結果データDATAは非特許文献4、及び、非特許文献5で定義される5-tuple形式のデータである。演算結果データDATAのsubjectフィールドの値がステップ1201において受信した公開鍵PUBLICKEY_AのSHA-1アルゴリズムによるハッシュ値HASH_Aと完全一致しているACLエントリが、ステップ1203において取得したアクセスコントロールリスト(ACL)に含まれる場合に限り、図10中のデータDATAのtagフィールドには図9のデータTAGと完全一致する文字列が含まれる。

[0038] 仲介装置(S)104は、出力された図10のデータDATAのtagフィールドを参照して、DNSクエリQUERY'を生成する(ステップ1207)。次に、DNSクエリQUERY'をドメインネームサーバ(DNS)105に提示して検索し、IPアドレスIPADDRESS_Bを取得する(ステップ1208)。次に、公開鍵PUBLICKEY_Aのハッシュ値HASH_Aをもとにアクセスコントロールリスト ACLを検索し、(subjectフィールドの値にハッシュ値HASH_Aと完全一致する文字列を含む(ACL)エントリENTRYを取得する(ステップ1209)。次に、ステップ1209において取得したACLエントリENTRYのtagフィールドを参照して、プライベートIPアドレスIPADDRESS_C及び属性情報ATTRIBUTE_Aを取得する(ステップ1210)。次に、VPNクライアント装置(A)101のIPアドレスIPADDRESS_Aを取得する(ステップ1211)。次に、共通鍵KEY_ABを生成する(ステップ1212)。

[0039] 図6に戻り、仲介装置(S)104は、ステップ1101において暗号化された通信路を用いて、上記取得したIPアドレスIPADDRESS_B、プライベートIPアドレスIPADDRESS_C、及び、生成した共通鍵KEY_ABをVPNクライアント装置(A)101に送信する(ステップ1104)。次に、クライアント装置(A)101と仲介装置(S)104は、接続を切断する(ステップ1105)。

次に、VPNゲートウェイ装置(B)103と仲介装置(S)104は、IPsecトランスポートモード

により接続する(ステップ1106)。すなわち、VPNゲートウエイ装置(B)103と仲介装置(S)104との間の通信路が暗号化される。次に、仲介装置(S)104は、ステップ1106において暗号化された通信路を用いて、先に取得したIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A及び、先にて生成した共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信する(ステップ1107)。次に、VPNゲートウェイ装置(B)103と仲介装置(S)104は、接続を切断する(ステップ1108)。

[0040] その後、図2に示したようなVPNゲートウェイ装置(B)103を経由して、クライアント装置(A)101から通信装置(C)111にIPsecトンネルモードによるリモートアクセスVPNが実行されるが、その詳細は省略する。

次に、VPNクライアント装置(A)101において証明書CERTを発行し、発行した証明書CERTをVPNクライアント装置(D)102に渡す手順を以下に示す。なお、その処理フロー図は省略する。

(1)VPNクライアント装置(A)101は、SPKI方式において定義された文法に従い、証明書CERTの証明書情報INFOを生成する。本実施例における証明書CERTの実施例を図11に示す。図11において、証明書情報INFOにおけるissuerフィールドの値は、公開鍵PUBLICKEY_Aの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_Aであると定義する。かつ、subjectフィールドの値は、公開鍵PUBLICKEY_DのSHA-1アルゴリズムによるハッシュ値HASH_Dであると定義する。かつ、tagフィールドの値は、VPNゲートウェイ装置Bに割り当てられたIPアドレスIPADDRESS_Bであると定義する。かつ、delegationフィールドの値は、非特許文献5において定義される文字列"propagate"であると定義する。一方、validityフィールドの値は、本発明とは直接関係しないため、任意の値を定義してもよい。

(2)VPNクライアント装置(A)101は、上記(1)において生成したデータに秘密鍵PRIVATEKEY_Aを用いて署名することにより、証明書CERTを発行する。

(3)VPNクライアント装置(A)101は、上記(2)において発行した証明書CERTを任意の手段でVPNクライアント装置(D)102にすべて送信する。

(4)VPNクライアント装置(D)102は、VPNクライアント装置(A)101から送信された証明書CERTを任意の手段ですべて受信し、記憶する。

[0041] 仲介装置(S)104が、VPNクライアント装置(D)102とVPNゲートウェイ装置(B)103との間のIKE等の認証に用いる共通鍵KEY_DBを生成し、次に、IPアドレスIPADDRESS_B、プライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_DBをVPNクライアント装置(D)102に送信し、次に、VPNクライアント装置(D)102に割り当てられたIPアドレスIPADDRESS_D、VPNクライアント装置(A)101の属性情報ATTRIBUTE_A、及び共通鍵KEY_DBをVPNゲートウェイ装置(B)103に送信する手順は、先の図6及び図7において説明した仲介装置(S)が、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103との間の共通鍵KEY_ABを生成して、IPアドレスIPADDRESS_B、プライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABをVPNクライアント装置(A)101に送信し、また、IPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信する手順と同様の手順で実施できる。

[0042] このようにして、図2に示したように、VPNゲートウェイ装置(B)103を経由して、VPNクライアント装置(D)102からも通信装置(C)111にIPsecトンネルモードによるリモートアクセスVPNが実行することが可能になる。

以上述べたように、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103より送信されたアクセスコントロールリスト(ACL)を記憶することで、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを記憶する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103だけが知っている、ローカルエリアネットワーク(LAN)110に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを知ることができる。従って、VPNクライアント装置(A)101は、VPNゲートウェイ装置(B)103を介した通信装置(C)111へのIPsecトンネルモードによるリモートアクセスVPNに必要なプライベートIPアドレスIPADDRESS_Cを、リモートアクセスVPNを実行する前に仲介装置(S)104に問い合わせることにより知ることができる。

[0043] また、本実施例において、仲介装置(S)104は、共通鍵KEY_ABを生成し、生成した共通鍵KEY_ABをVPNクライアント装置(A)101とVPNゲートウェイ装置(B)103の両者に送信する。これによって、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103はともに共通鍵KEY_ABを受信できる。従って、VPNクライアント装置(A)101とVPN

ゲートウェイ装置(B)103はIKEフェーズ1における認証に用いる共通鍵KEY_ABをオンラインで共有できる。

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを、仲介装置(S)104に記憶する。これによって、仲介装置(S)104は、偽装されていないVPNゲートウェイ装置(B)103から送信されたプライベートIPアドレスIPADDRESS_Cに限り記憶できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103から送信されたプライベートIPアドレスIPADDRESS_Cを知ることができる。

[0044] また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを記憶するという動作において、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信路を暗号化する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103から送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを改ざんされることなく、かつ、盗聴されることなく受信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103から送信された、通信装置(C)111に割り当てられた正しいプライベートIPアドレスIPADDRESS_Cを知ることができる。また、VPNゲートウェイ装置(B)103、通信装置(C)111に割り当てられた正しいプライベートIPアドレスIPADDRESS_Cを不特定多数に知られることなく仲介装置(S)104に送信できる。

[0045] また、本実施例において、仲介装置(S)104は、VPNクライアント装置(A)101を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bをドメインネームサーバ(DNS)105に問い合わせて取得し、共通鍵KEY_ABを生成し、取得したIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたIPアドレスIPADDRESS_C、及び、生成した共通鍵KEY_ABをすべてVPNクライアント装置(A)101に送信するという動作を実行する。これによって、仲介装置(S)104は、VPNクライアント装置(A)101が偽装されていない場合に限り、VPNゲー

トウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABのすべてをVPNクライアント装置(A)101に送信できる。従って、正しいVPNクライアント装置(A)101に限り、VPNゲートウェイ装置(B)103を介して、通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できる。

[0046] また、本実施例において、仲介装置(S)104は、VPNクライアント装置(A)101がVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを検索する権限を有しているか否かを判定し、権限を有している場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bをドメインネームサーバ(DNS)105に問い合わせて取得し、共通鍵KEY_ABを生成し、取得したIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたIPアドレスIPADDRESS_C、及び、生成した共通鍵KEY_ABをすべてVPNクライアント装置(A)101に送信するという動作を実行する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABのすべてを、VPNゲートウェイ装置(B)103、及び、通信装置(C)111に対しあらかじめアクセス権限を有するVPNクライアント装置(A)101だけに送信できる。従って、VPNゲートウェイ装置(B)103、及び、通信装置(C)111に対する、不特定多数からのIPsecトンネルモードによるリモートアクセスVPNを防止できる。

[0047] また、本実施例において、仲介装置(S)104は、仲介装置(S)104とVPNクライアント装置(A)101との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABを改ざんされることなく、かつ、盗聴されることなくVPNクライアント装置(A)101に送信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103を介して、正しい通信装置(C)111と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

[0048] また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証

し、認証に成功した場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信するという動作を実行する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103が偽装されていない場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103を介して、通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できるという効果が得られる。

[0049] また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信するという動作において、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信を暗号化するという動作を実行する。これによって、仲介装置(S)104は、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをすべて改ざんされることなく、かつ、盗聴されることなくVPNゲートウェイ装置Bに送信できる。従って、VPNゲートウェイ装置(B)103、及び、通信装置(C)111は、正しいVPNクライアント装置(A)101と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

[0050] また、本実施例において、仲介装置(S)104は、SPKI方式に従って、VPNクライアント装置(A)101、及び、VPNゲートウェイ装置(B)103を認証する。これによって、署名確認による本人性証明が可能なため、VPNクライアント装置(A)101及びVPNゲートウェイ装置(B)103の両者とも仲介装置(S)104に公開鍵証明書を送信する必要がなくなる。従って、VPNクライアント装置(A)101及びVPNゲートウェイ装置(B)103ともそれらの個人情報を仲介装置Sに対して隠蔽できる。

また、本実施例において、VPNクライアント装置(A)101は、SPKI方式に従って証明書CERTを発行し、VPNクライアント装置(D)102に送信する。これによって、VPNクライアント装置(A)101は、VPNクライアント装置(D)102に対して、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを検索する権限を委譲できるため、

VPNクライアント装置(D)102、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを検索することができる。かつ、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを知ることができる。従って、VPNクライアント装置(D)102も、VPNゲートウェイ装置(B)103を介して通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できるという効果が得られる。また、これによって、VPNゲートウェイ装置(B)103は他のVPNクライアント装置(D)102についての情報をアクセスコントロールリスト(ACL)に追加する必要なく、他のVPNクライアント装置(D)102からのリモートアクセスVPNを許可することができる。従って、VPNゲートウェイ装置(B)103は、アクセスコントロールリスト(ACL)の編集などの管理作業に要するコストを軽減できる。

[0051] なお、図1、図2に示すドメインネームサーバ(DNS)105において、公開鍵PUBLICKEY_Bのハッシュ値HASH_BとIPADDRESS_Bを関連付けて管理する場合、VPNゲートウェイ装置(B)103は公開鍵PUBLICKEY_Bのハッシュ値HASH_Bを生成してから、ハッシュ値HASH_BとIPアドレスIPADDRESS_BをドメインネームサーバDNSに登録し、かつ、図6に示す手順(ステップ1102)を、公開鍵PUBLICKEY_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_Bを含むDNSクエリQUERYに変更することにより明らかに実施できる。

また、図8に示すアクセスコントロールリスト(ACL)、図9に示すデータTAG、図10に示す演算結果のデータDATA、及び、図11に示す証明書CERTにおいて、SHA-1アルゴリズムの他の任意のハッシュ演算アルゴリズムを用いてハッシュ値HASH_Aを演算してもよい。また、issuerフィールドの値をハッシュ値HASH_Aの代わりに公開鍵PUBLICKEY_Aであると定義してもよい。同様に、subjectフィールドの値をハッシュ値HASH_Dの代わりに公開鍵PUBLICKEY_Dと定義してもよい。本変更を実施しても、SPKIに関する非特許文献4及び非特許文献5において定義される演算規則に従って演算することにより、アクセス制御に関して等しい実行結果が得られる。SHA-1アルゴリズム以外のハッシュ演算アルゴリズムを用いる場合の証明書CERTの形式、及び、issuerフィールド及びsubjectフィールドに公開鍵を指定する場合のアクセスコントロールリストACL、データDATA、及び、証明書CERTの形式については、SPKIに関す

る非特許文献5において詳細に説明されているため、その詳細な説明については省略する。本変更に伴い、図7に示す手順(ステップ1209)を公開鍵PUBLICKEY_Aを提示してアクセスコントロールリストACLを検索し、ACLエントリENTRYを取得する手順に変更することにより明らかに実施できる。

[0052] また、図2に示すVPNクライアント装置(A)101にはグローバルIPアドレスIPADDRESS_Aのみを割り当てているが、VPNクライアント装置(A)101とVPNゲートウェイ装置 (B)103 との間のIPsecトンネルモードのセットアップ時に、特許文献4、非特許文献1に示す方法等を用い、VPNクライアント装置(A)101に対してローカルエリアネットワークLAN内の任意のプライベートIPアドレスを、VPNゲートウェイ装置(B)103からの指示で動的に割り当ててもよい。また、仲介装置(S)104とVPNクライアント装置(A)101との間に設定されたIPsecトランスポートモードの通信路を通して、特許文献3に示す方法等を用いて、VPNクライアント装置(A)101に対してローカルエリアネットワークLAN内の任意のプライベートIPアドレスを、仲介装置(S)104からの指示で動的に割り当てても良い。

実施例2

本実施例は、証明書CERTについてさらに工夫し、証明書CERTをX.509形式の公開鍵証明書としたものである。基本的なシステム構成は先の実施例1と同様であるが、認証局が必要である。 図12に本実施例の全体的システム構成を示す。図12において、VPNクライアント装置(A)101、VPNゲートウェイ装置(B)103、認証局(CA)106、ドメインネームサーバ(DNS)105、及び、仲介装置(S)104はいずれもIP(Internet Protocol)に従ってネットワーク(WAN)100に接続されている。また、通信装置(C)111はVPNゲートウェイ装置(B)103をゲートウェイ装置とするローカルエリアネットワーク(LAN)110に接続されてる。

[0053] 図13は、図12の全体の動作を説明するための図である。太線はIPsecトンネルモードによるリモートアクセスVPN、点線はIKEフェーズ1における認証において、認証局(CA)106に公開鍵証明書CERTを提示することを示している。ここでも、VPNクライアント装置(A)101のホスト名は公開鍵PUBLICKEY_A(またはそのハッシュ値HASH_A)、IPアドレスはIPADDRESS_A、VPNゲードウェイ装置(B)103のホスト名は公開鍵

PUBLICKEY_B(またはハッシュ値HASH_B)、IPアドレスはIPADDRESS_B、通信装置(C)111のプライベートIPアドレスはIPADDRESS_Cとする。

[0054] VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、及び、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bはいずれもインターネットワーク(WAN)100内で一意であり、任意の手段で割り当てられる。VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY_B(またはそのハッシュ値HASH_B)とIPアドレスIPADDRESS_Bはドメインネームサーバ(DNS)105において一意に関連付けて管理される。通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cはローカルエリアネットワーク(LAN)110においてのみ一意であり、DHCP(Dynamic Host Configuration Protocol)、IPCP(PPP IP control protocol)等の任意の手段を用いて動的に割り当てられる。

[0055] VPNクライアント装置(A)101、VPNゲートウェイ装置(B)103、及び、仲介装置(S)104は、いずれも、IPsecトランスポートモード、または、IPsecトンネルモードにより通信路を暗号化する手段を有する。公開鍵PUBLICKEY_Aの秘密鍵はPRIVATEKEY_Aで、VPNクライアント装置(A)101で保管される。CERT_Aは、秘密鍵PRIVATEKEY_Aと対となる公開鍵PUBLICKEY_Aを含むX.509形式の公開鍵証明書で、認証局(CA)106の秘密鍵PRIVATEKEY_Rで署名され、VPNクライアント装置(A)101で保管される。また、公開鍵PUBLICKEY_Bの秘密鍵PRIVATEKEY_Bは、VPNゲートウェイ装置(B)103で保管される。CERT_Bは、秘密鍵PRIVATEKEY_Bと対となる公開鍵PUBLICKEY_Bを含むX.509形式の公開鍵証明書で、同じく認証局(CA)106の秘密鍵PRIVATEKEY_Rで署名され、VPNゲートウェイ装置(B)103で保管される。認証局(CA)106は、PKI(Public Key Infrastructure)方式に従い、VPNクライアント装置(A)101の公開鍵証明書CERT_A、及び、VPNゲートウェイ装置(B)103の公開鍵証明書CERT_Bを認証する。また、アクセスコントロールリスト(ACL)は、公開鍵PUBLICKEY_A及び公開鍵PUBLICKEY_Bの組み合わせに対して、プライベートIPアドレスIPADDRESS_C及びVPNクライアント装置(A)101の属性情報ATTRIBUTE_Aを関連付けたデータで、実施例1の図8と同様な構造を持ち、VPNゲートウェイ装置(B)103で保管される。また、秘密鍵PRIVATEKEY_Sは、仲介装置(S)104で保管される。

CERT_Sは、秘密鍵PRIVATEKEY_Sと対となる公開鍵PUBLICKEY_Sを含むX.509形式の公開鍵証明書で、認証局(CA)106の秘密鍵PRIVATEKEY_Rで署名され、仲介装置(S)104で保管される。

[0056] 仲介装置(S)104の構成は図3に示した実施例1における仲介装置(S)104の構成とほぼ同様であり、異なる点は、認証／アクセス権限制御手段1042がクライアント装置(A)及びゲートウェイ装置(B)の認証を認証局(CA)106によって署名されたクライアント装置(A)及びゲートウェイ装置(B)の公開鍵証明書CERT_A, CERT_Bによって行うことである。従って、仲介装置(S)104の構成の説明は省略し、以下の説明において仲介装置(S)104については図3を参照する。

IPアドレス取得手段1043は、DNS方式と呼ばれるインターネットにおける一般的な名前解決方式に従って、公開鍵PUBLICKEY_BからIPアドレスIPADDRESS_Bを検索する。ACL記憶手段1041は、公開鍵PUBLICKEY_Bと関連付けてアクセスコントロールリスト(ACL)を管理する。認証／アクセス権限制御手段1042は、公開鍵証明書CERT_Aに含まれる公開鍵PUBLICKEY_Aをアクセスコントロールリスト ACLに提示して検索し、検索結果として、公開鍵PUBLICKEY_A及び公開鍵PUBLICKEY_Bの組み合わせに対して一意に関連付けられたプライベートIPアドレスIPADDRESS_C及び属性情報ATTRIBUTE_Aを出力する。また、鍵生成手段1044は、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103との間のIKEフェーズ1における認証に用いる共通鍵KEY_ABを生成する。

[0057] 次に、図13を参照して、図12の動作概要を説明する。

アクセスコントロールリスト(ACL)の登録(記憶)時、VPNゲートウェイ装置(B)103は、公開鍵PUBLICKEY_B(またはそのハッシュ値HASH_B)とアクセスコントロールリスト(ACL)を仲介装置(S)104に送信する(ステップS21)。仲介装置(S)104は該公開鍵PUBLICKEY_B(またはそのハッシュ値HASH_B)と関連付けてアクセスコントロール(ACL)を図4A、図4Bの表として記憶する。VPNゲートウェイ装置(B)103を経由して、VPNクライアント装置(A)101から通信装置(C)111にIPsecトンネルモードによるリモートアクセスVPNを実行する場合、VPNクライアント装置(A)101は、公開鍵PUBLICKEY_Aと公開鍵PUBLICKEY_B(またはそのハッシュ値HASH_B)を仲介装置

(S)104に送信して、VPNゲートウェイ装置(B)103及び通信装置(C)のIPアドレスの検索要求を行なう(ステップS22)。

[0058] 仲介装置(S)104において、認証／アクセス権限制御手段1042はPKI方式に従ってVPNクライアント装置(A)101のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ(DNS)105を検索してVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを取得する(ステップS23)。また、仲介(S)104は、アクセスコントロール(ACL)を参照して、VPNゲートウェイ装置(B)103により管理されるLAN110に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C及び属性情報ATTRIBUTE_Aを取得する。さらに、仲介装置(S)104は、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)との間の認証に用いる共通鍵KEY_ABを生成する。そして、仲介装置(S)104は、仲介装置(S)104とVPNクライアント装置(A)101との間の通信路を暗号化し、VPNクライアント装置(A)101へIPADDRESS_B、IPADDRESS_C及び共通鍵KEY_ABを送信する(ステップS24)。また、仲介装置(S)104は、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信路を暗号化し、VPNゲートウェイ装置(B)103へIPADDRESS_AとATTRIBUTE_A、及びKEY_ABを送信する(ステップS25)。

[0059] 以上、図12に示すシステムの各装置の構成及び全体の動作概要を述べたが、ドメインネームサーバ(DNS)105におけるIPアドレスの管理及び名前解決方法、及び、IPsecトランスポートモードまたはトンネルモードによる通信路の暗号化方法、共通鍵KEY_ABの生成方法、及び、PKI方式によるX.509形式の公開鍵証明書CERT_A及びCERT_Bの認証方式については、当業者にとってよく知られているので、その詳細な構成は省略する。

以下に、本実施例2におけるアクセスコントロールリスト(ACL)の記憶手順、及びIPアドレスの取得、共通鍵の生成、これらIPアドレスと共通鍵の送信手順について詳述する。

[0060] まず、図14及び図15を参照して、VPNゲートウェイ装置(B)103において保管されるアクセスコントロールリスト(ACL)を仲介装置(S)104に記憶する手順について説明する。

図14において、VPNゲートウェイ装置(B)103と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1301)。IKEフェーズ1における認証はPKI方式に従い、VPN ゲートウェイ装置(B)103は公開鍵証明書CERT_Bを送信し、仲介装置(S)104は公開鍵証明書CERT_Sを送信する。VPNゲートウェイ装置(B)103は受信した公開鍵証明書CERT_Sを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は受信した公開鍵証明書CERT_Bを認証局CAに問い合わせて、公開鍵証明書CERT_Bの正しさをPKI方式に従って認証する。

[0061] VPNゲートウェイ装置(B)103は、ステップ1301において暗号化された通信路を用いて、アクセスコントロールリスト(ACL)をすべて送信する(ステップ1302)。仲介装置(S)104は、VPNゲートウェイ装置(B)103から送信されたアクセスコントロールリスト(ACL)を登録する(ステップ1303)。その後、VPNゲートウェイ装置(B)103と仲介装置(S)104は、接続を切断する(ステップ1304)。

図15は仲介装置(S)104でのアクセスコントロールリスト(ACL)の登録手順の詳細フローである。仲介装置(S)104は、まずVPNゲートウェイ装置(B)103から送信されたアクセスコントロールリスト(ACL)をすべて受信する(ステップ1401)。次に、先のステップ1301におけるIKE認証で用いた公開鍵証明書 CERT_Bを参照して、公開鍵PUBLICKEY_Bを取得する(ステップ1402)。次に、この取得した公開鍵PUBLICKEY_Bとステップ1401で受信したアクセスコントロールリストACLを関連づけて記憶する (ステップ1403)。

[0062] 次に、図16及び図17を参照して、仲介装置(S)104が、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103との間の共通鍵KEY_ABを生成し、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABをVPNクライアント装置(A)101に送信し、また、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信する手順について説明する。

[0063] 図16において、VPNクライアント装置(A)101と仲介装置(S)104は、IPsecトランスポ

ートモードにより接続する(ステップ1501)。IKEフェーズ1における認証はPKI方式に従い、VPN クライアント装置(A)101は公開鍵証明書CERT_Aを送信し、仲介装置(S)104は公開鍵証明書CERT_Sを送信する。VPNクライアント装置(A)101は受信した公開鍵証明書CERT_Sを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は受信した公開鍵証明書CERT_Aを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Aの正しさをPKI方式に従って認証する。

[0064] VPNクライアント装置(A)101は、ステップ1501において暗号化された通信路を用いて、VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY_Bを含むDNSクエリQUERYをすべて送信する(ステップ1502)。仲介装置(S)104は、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスにIPアドレスIPADDRESS_B、VPNゲートウェイ装置(B)103により管理されるLAN110に接続される通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを取得し、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103との間のIKE等の認証に用いる共通鍵KEY_ABを生成する(ステップ1503)。図17はステップ1503の詳細処理フローである。

[0065] 図17において、仲介装置(S)104は、まず、VPNクライアント装置(A)101から送信されたDNSクエリQUERYをすべて受信して入力する(ステップ1601)。次に、入力したDNSクエリQUERYを参照して、公開鍵PUBLICKEY_Bをすべて取得する(ステップ1602)。次に、取得した公開鍵PUBLICKEY_Bをもとに、それに関連付けられたアクセスコントロールリスト(ACL)をすべて取得する(ステップ1603)。次に、先のステップ1501におけるIKEフェーズ1認証に用いた公開鍵証明書CERT_Aを参照して、公開鍵PUBLICKEY_Aをすべて取得する(ステップ1604)。次に、この取得した公開鍵PUBLICKEY_Aをもとにアクセスコントロールリスト(ACL)を検索し、プライベートIPアドレスIPADDRESS_Cを取得する(ステップ1605)。そして、プライベートIPアドレスIPADDRESS_Cが取得されたと判定し(ステップ1606)、いかなるIPアドレスも取得できない場合には終了する。

[0066] プライベートIPアドレスIPADDRESS_Cが取得されたなら、次に、仲介装置Sは、上記

ステップ1601において受信したDNSクエリQUERYをドメインネームサーバ(DNS)105に提示して、IPアドレスIPADDRSSS_Bを取得する(ステップ1607)。VPNクライアント装置AのIPアドレスIPADDRESS_Aを取得する(ステップ1608)。共通鍵KEY_ABを生成する(ステップ1609)。

図16に戻り、仲介装置(S)104は、ステップ1501おいて暗号化された通信路を用いて、ステップ1607で取得したIPアドレスIPADDRESS_B、ステップ1605で取得したプライベートIPアドレスIPADDRESS_C、及び、ステップ1609で生成した共通鍵KEY_ABをすべてVPNクライアント装置(A)101に送信する(ステップ1504)。次に、VPNクライアント装置(A)101と仲介装置(S)104は、接続を切断する(ステップ1505)。

[0067] 次に、VPNゲートウェイ装置(B)103と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1506)。IKEフェーズ1における認証はPKI方式に従い、VPNゲートウェイ装置(B)103は公開鍵証明書CERT_Bを送信し、仲介装置Sは公開鍵証明書CERT_Sを送信する。VPNゲートウェイ装置(B)103は、受信した公開鍵証明書CERT_Sを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は、受信した公開鍵証明書CERT_Bを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Bの正しさをPKI方式に従って認証する。

[0068] 仲介装置(S)104は、ステップ1506において暗号化された通信路を用いて、先のステップ1605において取得した属性情報ATTRIBUTE_A、先のステップ1608において取得したIPアドレスIPADDRESS_A、及び先のステップ1609において生成した共通鍵KEY_ABをすべてVPNゲートウェイ装置(B)103に送信する(ステップ1507)。VPNゲートウェイ装置(B)103と仲介装置(S)104は、接続を切断する(ステップ1508)。

以上述べたように、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを記憶することで、仲介装置(S)104は、VPNゲートウェイ装置(B)103だけが知っている、ローカルエリアネットワーク(LAN)に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを知ることができる。従って、VPNクライアント装置(A)101は、VPNゲートウェイ装置(B)103を介した通信装置(C)1

11へのIPsecトンネルモードによるリモートアクセスVPNに必要なプライベートIPアドレスIPADDRESS_Cを、リモートアクセスVPNを実行する前に仲介装置(S)104に問い合わせることにより知ることができる。

[0069] また、本実施例において、仲介装置(S)104は、共通鍵KEY_ABを生成し、生成した共通鍵KEY_ABをVPNクライアント装置(A)101とVPNゲートウェイ装置(B)103の両者に送信するこれによって、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103はともに共通鍵KEY_ABを受信できる。従って、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103はIKEフェーズ1における認証に用いる共通鍵KEY_ABをオンラインで共有できる。

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを、仲介装置(S)104に記憶する。これによって、仲介装置(S)104は、偽装されていないVPNゲートウェイ装置(B)103から送信されたプライベートIPアドレスIPADDRESS_Cに限り記憶できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103から送信されたプライベートIPアドレスIPADDRESS_Cを知ることができる。

[0070] また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを、仲介装置(S)104に記憶するという動作において、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103から送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを改ざんされることなく、かつ、盗聴されることなく受信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103から送信された、通信装置(C)111に割り当てられた正しいプライベートIPアドレスIPADDRESS_Cを知ることができるという効果が得られる。また、VPNゲートウェイ装置(B)103は、通信装置(C)111に割り当てられた正しいプライベートIPアドレスIPADDRESS_Cを不特定多

数に知られることなく仲介装置(S)104に送信できる。

[0071] また、本実施例において、仲介装置(S)104は、VPNクライアント装置(A)101を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bをドメインネームサーバ(DNS)105に問い合わせて取得し、共通鍵KEY_ABを生成し、取得したIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたIPアドレスIPADDRESS_B、及び、生成した共通鍵KEY_ABをすべてVPNクライアント装置(A)101に送信する。これによって、仲介装置(S)104は、VPNクライアント装置(A)101が偽装されていない場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABのすべてをVPNクライアント装置(A)101に送信できる。従って、正しいVPNクライアント装置(A)101に限り、VPNゲートウェイ装置(B)103を介して、通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できる。

[0072] また、本実施例において、仲介装置(S)104は、VPNクライアント装置(A)101がVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを検索する権限を有しているか否かを判定し、権限を有している場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bをドメインネームサーバ(DNS)105に問い合わせて取得し、共通鍵KEY_ABを生成し、取得したIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたIPアドレスIPADDRESS_B、及び、生成した共通鍵KEY_ABをVPNクライアント装置(A)101に送信する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)101に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABのすべてを、VPNゲートウェイ装置(B)103、及び、通信装置(C)111に対しあらかじめアクセス権限を有するVPNクライアント装置(A)101だけに送信できる。従って、VPNゲートウェイ装置(B)103、及び、通信装置(C)111に対する、不特定多数からのIPsecトンネルモードによるリモートアクセスVPNを防止できる。

[0073] また、本実施例において、仲介装置(S)104は、仲介装置(S)104とVPNクライアント装置(A)101との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNゲ

ートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABを改ざんされることなく、かつ、盗聴されることなくVPNクライアント装置(A)に送信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103を介して、正しい通信装置(C)111と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

[0074] また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103が偽装されていない場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信できる。従って、VPNクライアント装置Aは、正しいVPNゲートウェイ装置(B)103を介して、通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できる。

[0075] また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信するという動作において、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、属性情報ATTRIBUTE_A、及び共通鍵KEY_ABをすべて改ざんされることなく、かつ、盗聴されることなくVPNゲートウェイ装置(B)103に送信できる。従って、VPNゲートウェイ装置(B)103、及び、通信装置(C)111は、正しいVPNクライアント装置(A)101と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

[0076] また、本実施例において、仲介装置(S)104は、PKI方式に従って、VPNクライアント装置(A)101及びVPNゲートウェイ装置(B)103を認証する。これによって、VPNクライアント装置(A)101の公開鍵証明書CERT_AもVPNゲートウェイ装置(B)103の公開鍵

証明書CERT_Bも仲介装置(S)104に送信することにより認証できる。従って、VPNクライアント装置(A)101の個人情報をVPNゲートウェイ装置(B)103に対して隠蔽できる。同様に、VPNゲートウェイ装置(B)103の個人情報をVPNクライアント装置(A)101に対して隠蔽できる。

[0077] なお、本実施例における図12、図13に示すドメインネームサーバ(DNS)105において、公開鍵PUBLICKEY_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_Bと IPADDRESS_Bを関連付けて管理する場合、VPNゲートウェイ装置(B)102は公開鍵PUBLICKEY_Bのハッシュ値HASH_Bを生成してから、ハッシュ値HASH_BとIPアドレスIPADDRESS_Bをドメインネームサーバ(DNS)105に登録すればよい。また、図16に示す手順のステップ1502を、公開鍵PUBLICKEY_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_Bを含むDNSクエリQUERYに変更することにより明らかに実施できる。

[0078] また、アクセスコントロールリスト(ACL)において、公開鍵PUBLICKEY_AとIPアドレスIPADDRESS_Cを関連付けて管理する代わりに、公開鍵PUBLICKEY_Aの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_AとIPアドレスIPADDRESS_Cと関連付けて管理しても良い、本変更に伴い、図14に示す手順のステップ1302において、VPNゲートウェイ装置(B)103は公開鍵PUBLICKEY_Aのハッシュ値HASH_Aを生成してから、ハッシュ値HASH_AとIPアドレスIPADDRESS_Cをアクセスコントロールリスト(ACL)として関連付けたデータを送信することにより明らかに実施できる。かつ、図17に示す手順のステップ1605を公開鍵PUBLICKEY_Aのハッシュ値HASH_Aを生成し、ハッシュ値HASH_Aを提示してアクセスコントロールリストACLを検索する手順に変更することにより、明らかに実施できる。

[0079] また、VPNクライアント装置(A)101にはグローバルIPアドレスIPADDRESS_Aのみを割り当てているが、これに加えて、仲介装置(S)104において、非特許文献1に示す方法等を用いてローカルエリアネットワークLAN内の任意のプライベートIPアドレスを割り当てても良い。

実施例3

前述の実施例1及び実施例2におけるVPNクライアント装置の実用的な機能構成を

図18に示す。 VPNクライアント装置101には、この装置から出されるDNS要求を捕捉し、代理応答するDNS問い合わせ捕捉・代理応答機能部1011、本発明の仲介サービスのVPNクライアント機能を実行する仲介サービス用VPNクライアント機能部1012、VPNアクセスを行うためのトンネリング・プロトコル機能部1013が設けられている。また、一般のDNS問い合わせと仲介サービスに関わるものとを識別し、管理するための仲介サービス管理テーブル1014、仲介サーバとの相互認証を行うための仲介サービス用認証情報1015、また、VPNゲートウェイとの間の暗号化通信を行うためのトンネリング・プロトコル構成管理情報1016が設けられている。

[0080] 仲介サービス用管理テーブル1014には、

a) 仲介サービス用Postfix: 仲介サービスに転送されるドメイン名（例：*.vpn）、

b) 仲介装置IPアドレス又はホスト名：仲介装置のIPアドレス、

c) 仲介装置との認証方式（SPKI方式、PKI方式、チャレンジレスポンス方式、鍵共有方式など）、

d) 認証に用いる証明書などの名称（認証方式に対応した証明書・秘密データを参照）、

が記録されている。

[0081] 仲介サービス用認証情報テーブル1015には、

a) VPNゲートウェイ装置検索に使われるドメイン名と対応するハッシュ値のテーブル、

b) VPNクライアント装置のクライアント認証のために利用される各種証明書類（SPKI証明書、PKI証明書、パスワード、共通鍵など）、

c) 仲介装置をサーバ認証する際に利用される証明書（SPKI証明書、PKI証明書、パスワード、共通鍵など）、

が記録されている。

[0082] トンネリング・プロトコル構成管理テーブル1016には、大きく分けて、

(1) トンネルをセットアップするための構成管理情報、

(2) セットアップされたトンネルの仮想ネットワークインタフェース(Nw.I/F)としての構成管理情報、

の2種類がある。以下にその詳細例を示す。

(1) トンネルをセットアップするための構成管理情報

A) トンネル起点のIPアドレス(VPNクライアント装置にネットワークから付与されたIPアドレス)。

[0083] B) トンネル終点のIPアドレス(VPNゲートウェイ装置にネットワークから付与されたIPアドレス。

C) トンネリングのプロトコル(IPsecトンネルモード、PPP over IPsecなど)。

D) 認証方式(SPKI方式、PKI方式、チャレンジレスポンス方式、鍵共有方式など)。

E) 認証に用いる証明書などの名称(認証方式に対応した証明書・秘密データを参照)。

(2) セットアップされたトンネルのネットワークインタフェース(Nw.I/F)としての構成管理情報

a) 仮想Nw.I/Fの種別(仮想PPP, 仮想イーサなど)、

b) 仮想Nw.I/FのIPアドレス、

c) ゲートウェイ、DNSサーバ、WINSサーバなどのIPアドレス、

d) 仮想Nw.I/Fへのルーティング情報。

このうち、仲介装置から通知されるものは:

(1) の設定項目のうち、B)。加えてC), D), E) もあってもよい。

[0084] (2) の設定項目B), C), D)のうち、VPNゲートウェイ装置から動的に通知しないもの(仲介装置とVPNゲートウェイ装置のどちらかでも通知すればよい。)

本実施例での仲介処理は以下のようにして行われる。

まず、アプリケーションから、通信に先立って、アクセスしたいVPNサービスを提供しているVPNゲートウェイ装置のIPアドレスを問い合わせるDNS問い合わせ要求が出される(ステップS1)。

この要求は、DNS問い合わせ捕捉・代理応答機能部1011により一旦捕捉され、これが仲介サービスに関わるものか仲介サービス用管理テーブル1014を参照して識別される。もし、仲介サービスに関係ないものであれば、一般のDNS問い合わせ要求とし

てDNSサーバ105に対し通常のDNS処理が実行されその応答からIPアドレスを得て一般の接続処理が行われる(ステップS2)。

[0085] もし、仲介サービスに関わるものであれば、そのDNS問い合わせ要求は、仲介サービス用VPNクライアント機能部1012に転送される(ステップS3)。

仲介サービス用VPNクライアント機能部1012では、仲介サービス用管理テーブル1014の内容に従い、所定の仲介サーバを選択し(ステップS4)、仲介サービス用認証情報テーブル1015を用いて相互認証を行う(ステップS5)。

次に仲介装置104に前述の実施例で説明した仲介要求を出し(ステップS6)、その応答を得る(ステップS7)。この情報をもとに、トンネリング・プロトコル構成管理テーブル1016中のVPNゲートウェイアドレス、共通鍵などの情報を更新し(ステップS8)、まだ、所定のトンネルが張られていなければ、トンネルセットアップ要求をトンネリング・プロトコル部1013に対して出す(ステップS9)。

[0086] トンネリング・プロトコル部1013は、トンネリング・プロトコル構成管理テーブル1016を参照してトンネルの相手側であるVPNゲートウェイ装置103を識別し(ステップS10)、また、本仲介機能により設定された共通鍵を利用して、VPNゲートウェイ装置103との間に暗号化通信のトンネルをセットアップする(ステップS11)。

トンネルが正常にセットアップされると、VPNクライアント装置101のプライベートIPアドレス、内部DNSやルーティング関連情報などの構成管理情報の一部が、特許文献4、非特許文献1、非特許文献2、非特許文献3記載の方法を用いて、VPNゲートウェイ装置103から動的に渡されうる。この場合、それらの情報を用いて、トンネリング・プロトコル構成管理テーブル1016を更新し(ステップS12)、トンネルセットアップ完了の応答を仲介サービス用VPNクライアント機能部1012に返す(ステップS13)。

[0087] 仲介サービス用VPNクライアント機能部1012は、VPNトンネルのセットアップが正常に完了した場合、ステップS7で取得した通信装置のプライベートIPアドレスをDNS問い合わせへの応答として、DNS問い合わせ捕捉・代理応答機能部1011に返す(ステップS14)。この応答は、そのまま、DNS問い合わせを発したアプリケーションに返される(ステップS15)。アプリケーションは、設定されたVPNトンネルを経由して、VPN通信を行う(ステップS16)。

実施例4　この発明が適用されたシステム全体の構成例を図19に示す。本実施例では、VPNクライアント装置101、102は人事部用と経理部用の2台であり、それぞれ、公開鍵ハッシュ値A1、A2を持つとする。また、VPNゲートウェイ装置103が管理するVPNは、人事部用VLAN121と経理部用VLAN122があり、VPNゲートウェイ装置103は、イーサスイッチ123を介してIEEE 802.1Q VLANタグ多重化により両VLAN121、122と接続されているとする。また、仲介装置104には、本VPNゲートウェイ装置103のため、図20に示すアクセスコントロールリスト(ACL)が予めアップロードされているとする。このACLでは、ハッシュ値 HASH_A1 の公開鍵を持つVPNクライアント装置101は、属性情報"(VLAN 人事部VLAN)"を持ち、また、ハッシュ値HASH_A2の公開鍵をもつVPNクライアント装置102は、属性情報"(VLAN 経理部VLAN)"を持つと宣言されている。

[0088]　図21に本実施例におけるVPNゲートウェイ装置103の機能構成図を示す。VPNゲートウェイ装置103には、仲介装置104との通信・処理を行う仲介サービス用VPNゲートウェイ機能部1031と、複数のVPNクライアント装置からのトンネルを終端するトンネリング・プロトコル部1032と、トンネルから取り出されたデータパケットをVPN内の所定のVLANに収容し、またトンネルに出入りするパケットのうちセキュリティ上問題があるものを除去するフィルタリングするフィルタリング／VLAN多重機能部1033とが設けられている。また、仲介装置104との接続に必要な情報をもつ仲介サービス用管理テーブル1034と、仲介装置104との認証用の仲介サービス用認証情報テーブル1035と、VPNクライアント装置101、102との各トンネルに関する構成管理情報を保持するトンネリング・プロトコル構成管理テーブル1036と、VPNゲートウェイ装置103が管理する各VLANに関する構成管理情報を保持するVLAN構成管理テーブル1037とが設けられている。

[0089]　仲介サービス用管理テーブル1034には利用する仲介装置ごとに以下の情報が保持されている。

a) 仲介装置IPアドレス又はホスト名：仲介装置のIPアドレス。

b) 仲介装置との認証方式(SPKI方式、PKI方式、チャレンジレスポンス方式、鍵共有方式など)。

c) 認証に用いる証明書等の名称(認証方式に対応した証明書・秘密データを参照)。

仲介サービス用認証情報テーブル1035には以下の情報が保持されている。

[0090] a) VPNゲートウェイ装置の認証のために利用される各種証明書類(SPKI証明書、PKI証明書、パスワード、共通鍵など)。

b) 仲介装置を認証する際に利用される証明書(SPKI証明書、PKI証明書、パスワード、共通鍵など)。

トンネリング・プロトコル構成管理テーブル1036にはVPNクライアント装置とのトンネルごとに以下の情報が保持されている。

a) トンネル起点のIPアドレス(VPNクライアント装置にネットワークから付与されたIPアドレス)。

[0091] b) トンネリングのプロトコル(IPsecトンネルモード、PPP over IPsecなど)。

c) 認証・暗号化方式(SPKI1方式、PKI方式、チャレンジレスポンス方式、鍵共有方式など)。仲介サービスの結果、VPNゲートウェイ装置との間にセットアップされるトンネルは、鍵共有方式になる。

d) 認証に用いる証明書等の名称(認証方式に対応した証明書・秘密データを参照)

e) 仲介サービスから通知された共通鍵、及び属性情報。

f) トンネルが接続されるVLAN名称。"人事部VLAN"、"経理部VLAN"など。

[0092] g) VPNクライアント装置に払い出されてたプライベートIPアドレス(VLAN構成管理情報、d)の中から選択)。

VLAN構成管理テーブル1037にはVLAN内に存在するVLANごとに以下の情報を保持している。

a) VLAN名称("人事部VLAN"、"経理部VLAN"など)。

b) VLANのネットワーク構成管理情報。

i)ゲートウェイ、DNSサーバ、WINSサーバなどのIPアドレス。

[0093] ii) VPNクライアント装置に通知するルーティング情報。

c) 適用するパケットフィルタ条件(アクセス可能なサービスを限定)

d) VPNクライアント装置に払い出し可能なプライベートIPアドレス範囲。

本実施例におけるVPNゲートウェイ装置103の仲介処理は、以下のようにして行われる。

VPNゲートウェイ装置103は、仲介サービス用管理情報テーブル1034及び仲介サービス用認証情報テーブル1035を用いて、仲介装置104とのセキュアな通信路を確保し、VPNアクセス仲介要求を出す(ステップS1−S3)。仲介装置104は、例えばVPNクライアント装置101を認証すると、VPNゲートウェイ装置103に対し、VPNアクセス仲介通知を行う(ステップS4)。通知情報(VPNクライアント装置101のIPアドレスIPADDRESS_A1、共通鍵KEY_AB、属性情報ATTRIBUTE_A1など)は、トンネリング・プロトコル構成管理テーブル1036に格納される。また、属性情報をもとに、収容するVLAN121が決定され、そのVLAN名「人事部VLAN」も、このテーブルに格納される(ステップS5)。この場合、図20により、VPNクライアント装置101は、(VLAN人事部VLAN)の属性情報をもつことが通知される。従って、VPNクライアント装置101からのトンネルを収容するVLANは、”人事部VLAN”と決定される。

[0094] VPNクライアント装置101からのVPNトンネルセットアップ要求が出されると(ステップS6)、トンネリング・プロトコル構成管理テーブル1036を参照して(ステップS7)、所定の認証・暗号化を行った後、対応するVLAN121のVLAN構成管理テーブル1037を参照(ステップS8)して、VPNクライアント装置101に払い出し可能なプライベートIPアドレス範囲から未使用なものを選択し、ネットワーク構成管理情報(ゲートウェイ、DNS, WINSサーバなどのアドレスなど)とともに、VPNクライアント装置101に通知する。この場合、VPNクライアント装置101のプライベートIPアドレスは、人事部VLANのアドレスプールから払いだされる。また、ゲートウェイ、DNSなどのネットワーク構成管理情報も、人事部VLANNのものが通知される。

[0095] VPNクライアント装置101から上記トンネルを通してVPN向けデータパケットが到着すると、トンネルが収容されているVLANのフィルタ条件によりフィルタリングされた後、VLANへ転送される(ステップS10)。このほか、属性情報により、トンネルごとのフィルタリングを追加設定してもよい。VPNクライアント装置102からの要求も同様に処理する。

トンネルを切断する場合は、対応するエントリをトンネリング・プロトコル構成管理テーブル1036から除去し、VPNクライアント装置に割り当てられていたプライベートIPアドレスを所属VLANのアドレスプールに返却する。

以上説明したように、この発明によれば、仲介装置において、IPネットワークに接続したVPNクライアント装置、及び、VPNゲートウェイ装置と、VPNゲートウェイ装置により管理されるローカルエリアネットワークに接続した任意の通信装置との間のIPsec、L2TP等の任意のトンネリングプロトコルによるリモートアクセスVPNを確立するために用いる情報(コントロールアクセスリスト)を記憶する。この情報には、通信装置に割り当てられたプライベートIPアドレスが含まれる。

[0096] 仲介装置は、VPNクライアント装置からVPNゲートウェイ装置に割り当てられたIPアドレスの検索要求を受信したら、VPNクライアント装置がVPNゲートウェイ装置に割り当てられたIPアドレスを検索する権限を有するかどうかを検証する。そして、権限を有する場合に限り、アクセスコントロールリストを参照して、VPNゲートウェイ装置により管理されるローカルエリアネットワークに接続した通信装置に割り当てられたプライベートIPアドレス及びVPNクライアント装置の属性情報を取得し、ドメインネームサーバ(DNS)を検索してVPNゲートウェイ装置に割り当てられたIPアドレスを取得し、VPNクライアント装置とVPNゲートウェイ装置との間のIKE等の認証に用いる共通鍵を生成する。次に、仲介装置とVPNクライアント装置との間の通信路を暗号化して、VPNゲートウェイ装置に割り当てられたIPアドレス、通信装置に割り当てられたプライベートIPアドレス及び生成した共通鍵をVPNクライアント装置に送信する。また、仲介装置とVPNゲートウェイ装置との通信路を暗号化して、VPNクライアント装置に割り当てられたIPアドレス、生成した共通鍵及びクライアント装置の属性情報をVPNゲートウェイ装置に送信する。なお、VPNゲートウェイ装置のDNSクエリにおけるホスト名は、物理的なVPNゲートウェイ装置というより、当該装置を経由して提供されるVPNのポータルサービスとみなしてよい。このサービスは、プライベートIPアドレスをもつ通信装置から提供される。ひとつのVPNゲートウェイ装置に対して複数のホスト名を付与し、DNSに登録することで、異なるプライベートIPアドレスをもつ複数の通信装置を関連づけることができる。たとえば、取引先むけと社内向けのふたつの通信装置がVPNゲートウェイ装

置の管理するVPN内にある場合、異なるホスト名を付与することにより、異なるアクセスコントロールリストで管理し、取引先と社内のVPNアクセス装置をそれぞれに対応した通信装置に導いてもよい。

[0097] また、仲介装置は、SPKI方式に従って、VPNクライアント装置、及び、VPNゲートウェイ装置を認証する。また、VPNクライアント装置は、SPKI方式に従って証明書を発行する。さらに、仲介装置はPKI方式に従って、VPNクライアント装置、及び、VPNゲートウェイ装置を認証することも可能とする。

また、仲介装置は、公開鍵、FQDN(Fully Qualified Distinguished Name), GUID(Globally Unique Identifier), MACアドレス, SPKI(Simple Public Key Infrastructure) Local Name, X.500 Distinguish Name等の任意の名前形式に従ってVPNクライアント装置、VPNゲートウェイ装置、及び、通信装置を識別することも可能とする。これによって、IPsec、L2TPなどの任意のトンネリングプロトコル、PKI、SPKI、パスワードなどの任意の認証方式を組み合わせてリモートアクセスVPNを実行できる。

[0098] 上述した実施例1乃至実施例4で示したシステムにおける各装置の一部もしくは全部の処理機能をコンピュータのプログラムで構成し、そのプログラムをコンピュータを用いて実行して本発明を実現することができること、あるいは、実施例1や実施例2で示した処理手順をコンピュータのプログラムで構成し、そのプログラムをコンピュータに実行させることができることは言うまでもない。コンピュータでその処理機能を実現するためのプログラム、あるいは、コンピュータにその処理手順を実行させるためのプログラムを、そのコンピュータが読み取り可能な記録媒体、例えば、FD、MO、ROM、メモリカード、CD、DVD、リムーバブルディスクなどに記録して、保存したり、提供したりすることができるとともに、インターネット等のネットワークを通してそのプログラムを配布したりすることが可能である。

請求の範囲

[1] IPネットワークにバーチャルプライベートネットワーク、以下VPN、クライアント装置及びVPNゲートウェイ装置が接続され、VPNゲートウェイ装置により管理されるローカルエリアネットワークに通信装置が接続され、前記IPネットワークに接続された任意のVPNクライアント装置と、VPNゲートウェイ装置、及び、VPNゲートウェイ装置に管理されるローカルエリアネットワークに接続された任意の通信装置との間のトンネリングプロトコルによるリモートアクセスVPNを実行するシステムにおけるリモートアクセスVPN仲介方法であり、

(a) 前記IPネットワーク上に設けられた仲介装置に、前記VPNゲートウェイ装置から前記通信装置に割り当てられたプライベートIPアドレスを示す情報を含むアクセスコントロールリストを前記仲介装置に送信する過程と、

(b) 前記仲介装置で前記アクセスコントロールリストを前記VPNゲートウェイ装置に対応して記憶する過程と、

(c) 前記VPNクライアント装置からの要求に応答して前記VPNゲートウェイ装置に対応するIPアドレスを検索し、上記アクセスコントロールリストから対応する前記通信装置のプライベートIPアドレスを取得し、前記VPNクライアント装置に送ると共に、前記クライアント装置のIPアドレスを前記VPNゲートウェイ装置に送り、前記VPNクライアント装置と前記ゲートウェイ装置との間の認証された暗号化トンネルをセットアップするために用いる相互認証情報を生成し、前記VPNクライアント装置と前記ゲートウェイ装置の双方に送る過程と、

(d) 前記相互認証情報を用いて前記VPNクライアント装置と前記ゲートウェイ装置間で認証された暗号化トンネルセットアップを行い、この暗号化トンネルを通して前記通信装置のプライベートIPアドレスを使ってリモートアクセスを実行する過程、

とを含む。

[2] 請求項1記載のリモートアクセスVPN仲介方法において、前記アクセスコントロールリストは前記VPNクライアント装置に関する属性情報を含む。

[3] 請求項2記載のリモートアクセスVPN仲介方法において、前記過程(a) は、前記仲介装置と前記VPNゲートウェイ装置又はそれを管理する権限を有するVPNゲートウェ

イ管理装置との間の通信路を暗号化して、前記VPNゲートウェイ装置からアクセスコントロールリストを前記仲介装置に送信する過程を含む。

[4] 請求項2又は3記載のリモートアクセスVPN仲介方法において、前記過程(b)は、前記仲介装置が、前記VPNゲートウェイ装置等を認証する過程と、認証に成功した場合に、前記VPNゲートウェイ装置により送信された前記VPNクライアント装置に対するアクセスコントロールリストを記憶する過程とを含む。

[5] 請求項2又は3記載のリモートアクセスVPN仲介方法において、前記過程(c)は、

(c-0) 前記VPNクライアント装置から前記VPNゲートウェイ装置に割り当てられたIPアドレスの検索要求を受信したなら、前記VPNクライアント装置が前記VPNゲートウェイ装置のアクセス権限を有するかどうか検証する過程と、

アクセス権限を有する場合に限り、

(c-1) アクセスコントロールリストを参照して、通信装置に割り当てられたプライベートIPアドレスを取得する過程と、

(c-2) ドメインネームサーバを検索してVPNゲートウェイ装置に割り当てられたIPアドレスを取得する過程と、

(c-3) 仲介装置とVPNクライアント装置との通信路を暗号化して、VPNゲートウェイ装置のIPアドレス及び通信装置のプライベートIPアドレスをVPNクライアント装置に送信する過程と、

(c-4) 仲介装置とVPNゲートウェイ装置との通信路を暗号化して、VPNクライアント装置のグローバルIPアドレス及びアクセスコントロールリストに記載されたVPNクライアント装置に関する前記属性情報をVPNゲートウェイ装置に送信する過程、

とを含み、前記過程(d)は、

(d-1) VPNクライアント装置とVPNゲートウェイ装置との間の認証に用いる前記相互認証情報を生成する過程と、

(d-2) 仲介装置とVPNクライアント装置との通信路を暗号化して、VPNゲートウェイ装置との相互認証に必要な情報をVPNクライアント装置に送信する過程と、

(d-3) 仲介装置とVPNゲートウェイ装置との通信路を暗号化して、VPNクライアント装置との相互認証に必要な情報をVPNゲートウェイ装置に送信する過程、

とを含む。

[6] 請求項5記載のリモートアクセスVPN仲介方法において、前記VPNゲートウェイ装置が、VPNクライアント装置とVPNゲートウェイ装置との間の暗号化トンネルセットアップ時に、仲介装置から送信されたVPNクライアント装置に関する前記属性情報に基づいて、前記VPNクライアント装置に付与すべきプライベートIPアドレスを決定し付与する機能と、VPNクライアント装置に関する前記属性情報に基づいて収容するVLAN、ゲートウェイアドレス、内部DNSアドレス、WINSサーバアドレス、などを決定する機能と、前記属性情報に基づいて前記VPNゲートウェイ装置のパケットフィルタリング設定を変更する機能、の少なくとも1つを実行する過程と、

上記VPNゲートウェイ装置が、VPNクライアント装置との間に確立したトンネルが切断ないし無通信が所定の時間継続した場合に、トンネルのクリーンアップ処理、VPNクライアント装置に割り当てたプライベートIPアドレスの返却処理、当該VPNクライアント装置のために行った当該VPNゲートウェイ装置のパケットフィルタリング設定を復元する過程を含む。

[7] 請求項2又は3記載のリモートアクセスVPN仲介方法において、前記過程(c) は、VPNクライアント装置が、装置内アプリケーションあるいは、他VPNクライアント装置から転送されてきたDNS問い合わせを捕捉し、当該問い合わせのソースアドレスや問い合わせ内容をフィルタ条件と照合し、条件に合致した場合には、その問い合わせを上記仲介装置への問い合わせに変換する過程を含み、前記過程(d) は、その応答をもとにトンネリングプロトコルの構成管理情報を設定・更新する過程を含み、前記過程(e) は、必要に応じてトンネルを初期化し、DNS問い合わせ結果として仲介装置により指定された通信装置のプライベートIPアドレスを問い合わせもとのアプリケーションに問い合わせ結果として渡す過程を含む。

[8] 請求項5記載のリモートアクセスVPN仲介方法において、前記過程(c) は、前記VPNクライアント装置が、SPKI方式に従って証明書を発行し、前記証明書を受信した他のVPNクライアント装置が前記仲介装置に対して、前記VPNゲートウェイ装置に割り当てられたIPアドレスの検索要求を送信する過程を含む。

[9] IPネットワークにVPNクライアント装置及びVPNゲートウェイ装置が接続され、VPNゲ

ートウェイ装置により管理されるローカルエリアネットワークに通信装置が接続され、前記IPネットワークに接続された任意のVPNクライアント装置と、VPNゲートウェイ装置、及び、VPNゲートウェイ装置に管理されるローカルエリアネットワークに接続された任意の通信装置との間のトンネリングプロトコルによるリモートアクセスVPNを実行するシステムにおいて、IPネットワーク上に設置されて、リモートアクセスVPNの確立を仲介する仲介装置であって、

前記VPNゲートウェイ装置から送信される前記通信装置に割り当てられたプライベートIPアドレスを示す情報を含むアクセスコントロールリスト、以下ACL、を記憶するACL記憶手段と、

前記VPNクライアント装置、前記ゲートウェイ装置を認証し、アクセス権限制御を実行する認証／アクセス権限制御手段と、

前記アクセスコントロールリストを参照して、前記通信装置に割り当てられたプライベートIPアドレスを取得し、ドメインネームサーバを検索して前記VPNゲートウェイ装置に割り当てられたIPアドレスを取得するIPアドレス取得手段と、

前記VPNクライアント装置と前記VPNゲートウェイ装置との間の認証された暗号化トンネルをセットアップするために用いる相互認証情報を生成する認証情報生成手段と、

前記VPNクライアント装置に、前記VPNゲートウェイ装置のIPアドレス、前記通信装置のプライベートIPアドレス及び前記相互認証情報を送信し、前記VPNゲートウェイ装置に、前記VPNクライアント装置のIPアドレス及び前記相互認証情報を送信する通信手段、

とを含む。

[10] 請求項9記載の仲介装置において、前記通信手段は、仲介装置とVPNクライアント装置との間の通信、仲介装置とVPNゲートウェイ装置との間の通信を、それぞれ暗号化する暗号化手段を含む。

[11] 請求項9記載の仲介装置において、前記認証／アクセス権限制御手段は、前記VPNクライアント装置を認証し、認証に成功した場合に限り、前記IPアドレス取得手段に対し前記VPNゲートウェイ装置に割り当てられたIPアドレスをドメインネームサー

バに問い合わせて取得させ、前記相互認証情報生成手段に対し前記相互認証情報を生成させ、前記通信手段に、取得したIPアドレスと、前記通信装置に割り当てられたプライベートIPアドレス、及び生成した前記相互認証情報を前記VPNクライアント装置に送信させる。

[12] 請求項9記載の仲介装置において、前記認証／アクセス権限制御手段は前記VPNクライアント装置が前記VPNゲートウェイ装置に割り当てられたIPアドレスを検索する権限を有しているか否かを判定し、権限を有している場合に限り、前記IPアドレス取得手段に対し前記VPNゲートウェイ装置に割り当てられたIPアドレスをドメインネームサーバに問い合わせて取得させ、前記相互認証情報生成手段に対し前記相互認証情報を生成させ、前記通信手段に対し取得したIPアドレス、前記通信装置に割り当てられたプライベートIPアドレス、及び、生成した前記相互認証情報を前記VPNクライアント装置に送信させる。

[13] 請求項11又は12記載の仲介装置において、前記認証／アクセス権限制御手段は、前記VPNゲートウェイ装置を認証し、認証に成功した場合に限り、前記通信手段に対し前記VPNクライアント装置に割り当てられたIPアドレス、及び、前記相互認証情報を前記VPNゲートウェイ装置に送信させる。

[14] 請求項9乃至13のいずれかに記載の仲介装置において、前記認証／アクセス権限制御手段は、SPKI(Simple Public Key Infrastructure)方式に従って、前記VPNクライアント装置、及び、前記VPNゲートウェイ装置を認証し、及び／または、アクセ権限制御を実行する。

[15] 請求項9乃至13のいずれかに記載の仲介装置において、前記認証／アクセス権限制御手段は、PKI(Public Key Infrastructure)方式に従って、前記VPNクライアント装置、及び、前記VPNゲートウェイ装置を認証する。

[図1]

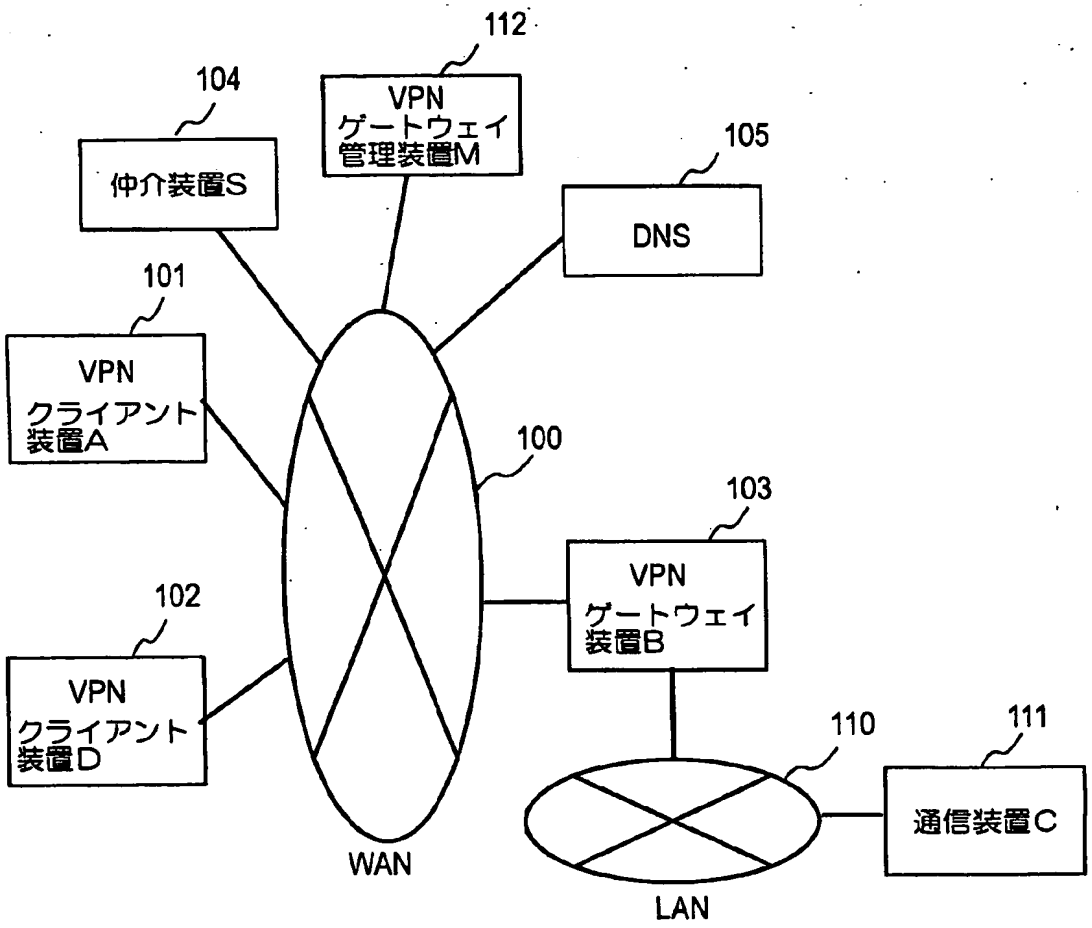

112
VPN
ゲートウェイ
管理装置M
104
仲介装置S
105
DNS
101
VPN
クライアント
装置A
100
103
VPN
ゲートウェイ
装置B
102
VPN
クライアント
装置D
110
111
通信装置C
WAN
LAN

図1

[図2]

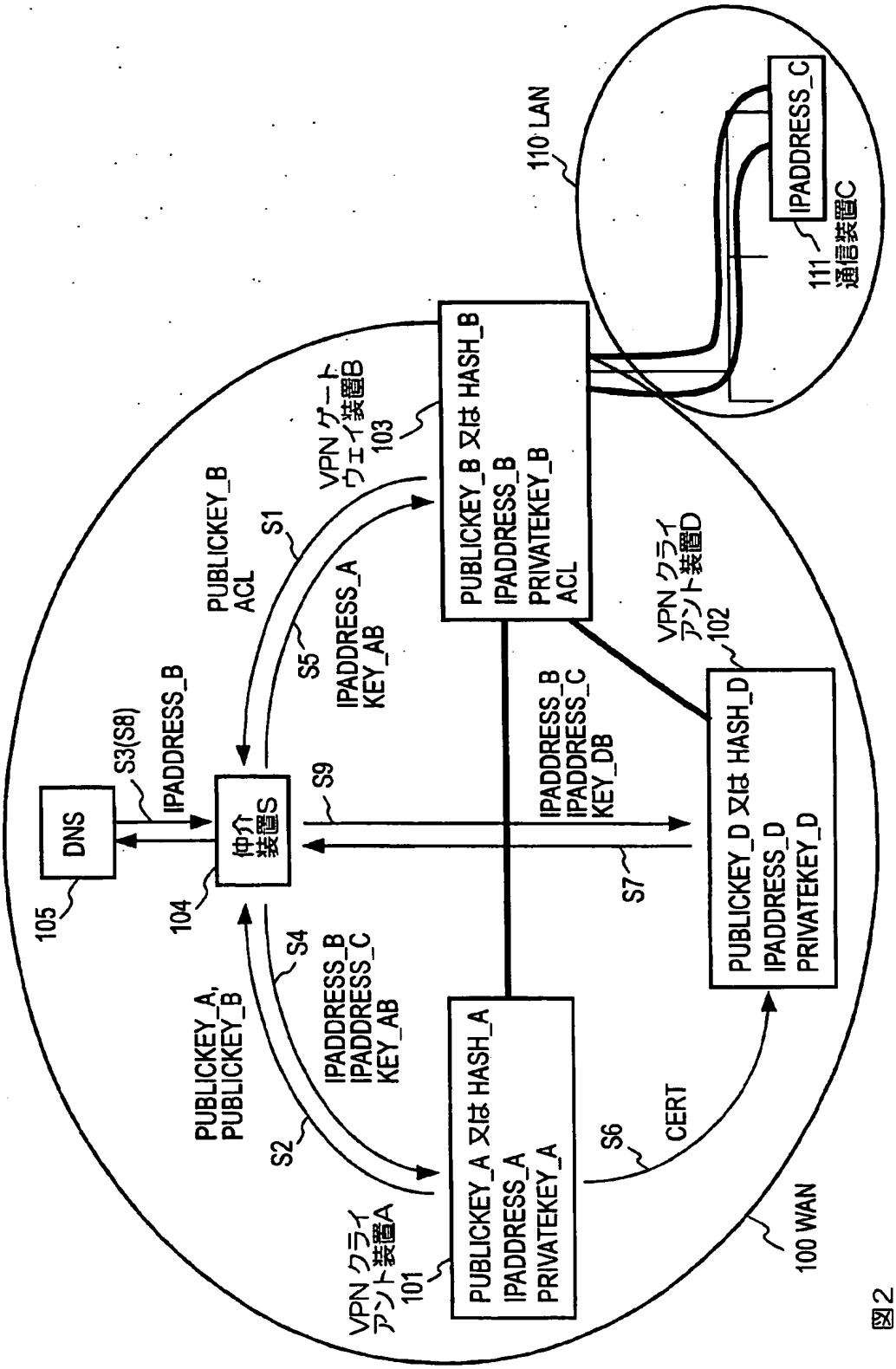

110 LAN
IPADDRESS_C
111
通信装置C
VPN ゲート
ウェイ装置B
103
PUBLICKEY_B 又は HASH_B
IPADDRESS_B
PRIVATEKEY_B
ACL
PUBLICKEY_B
ACL
S1
S5
IPADDRESS_A
KEY_AB
VPN クライ
アント装置D
102
IPADDRESS_B
IPADDRESS_C
KEY_DB
S3(S8)
IPADDRESS_B
DNS
105
仲介
装置S
104
S9
S7
PUBLICKEY_D 又は HASH_D
IPADDRESS_D
PRIVATEKEY_D
S4
IPADDRESS_B
IPADDRESS_C
KEY_AB
PUBLICKEY_A,
PUBLICKEY_B
S2
S6
CERT
PUBLICKEY_A 又は HASH_A
IPADDRESS_A
PRIVATEKEY_A
VPN クライ
アント装置A
101
100 WAN

図2

[図3]

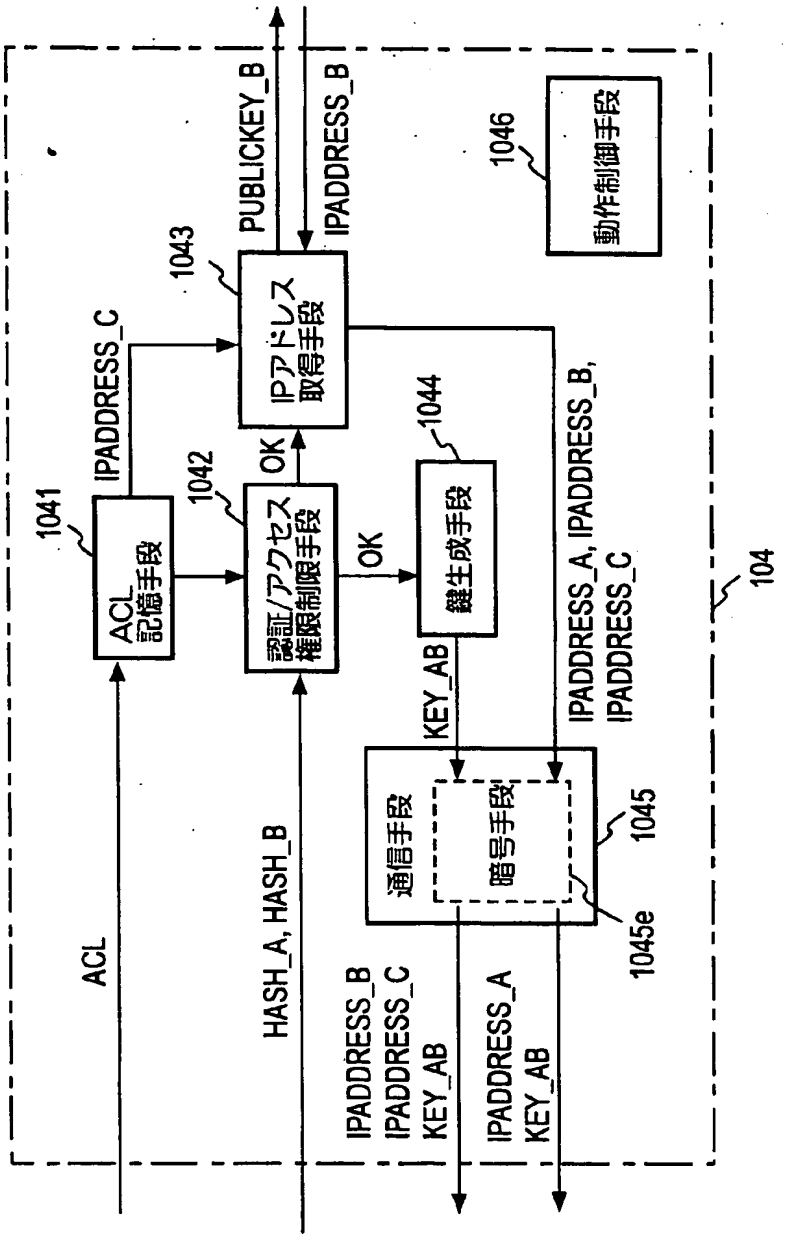

104
1041
ACL 記憶手段
1042
認証/アクセス権限制限手段
1043
IPアドレス取得手段
1044
鍵生成手段
1045
通信手段
暗号手段
1045e
1046
動作制御手段
IPADDRESS_C
PUBLICKEY_B
IPADDRESS_B
OK
OK
KEY_AB
IPADDRESS_A, IPADDRESS_B, IPADDRESS_C
ACL
HASH_A, HASH_B
IPADDRESS_B
IPADDRESS_C
KEY_AB
IPADDRESS_A
KEY_AB

図3

[図4]

図4A

1041T

HASH_B	ACL
HASH_B1	ACL1
HASH_B2	ACL2
⋮	⋮

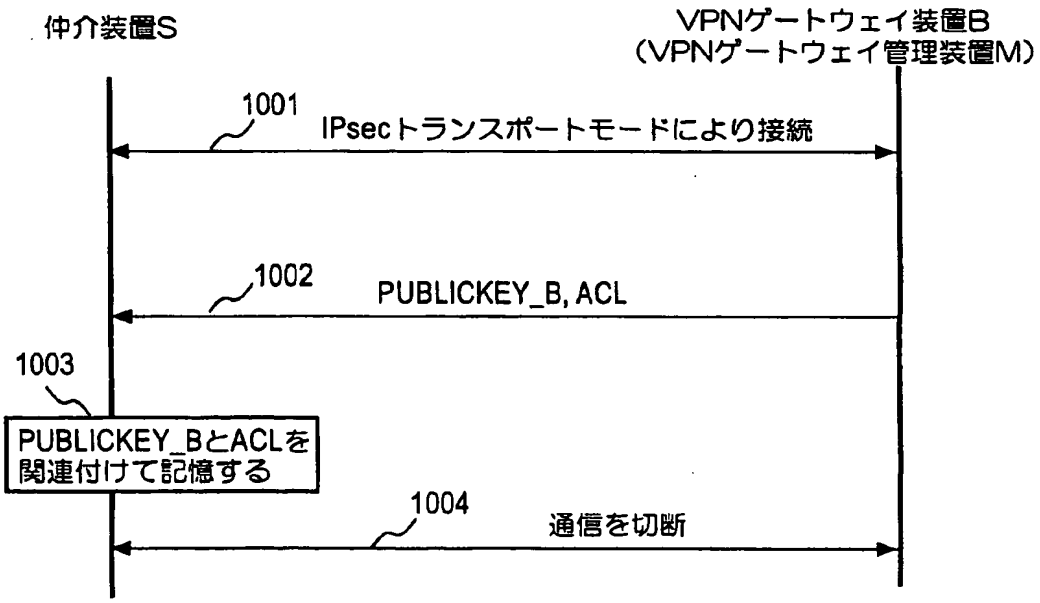
図4B

ACL1

アクセス対象	アクセス主体
IPADDRESS_C1	HASH_A
IPADDRESS_C2	HASH_D
⋮	⋮

[図5]

図5



[図6]

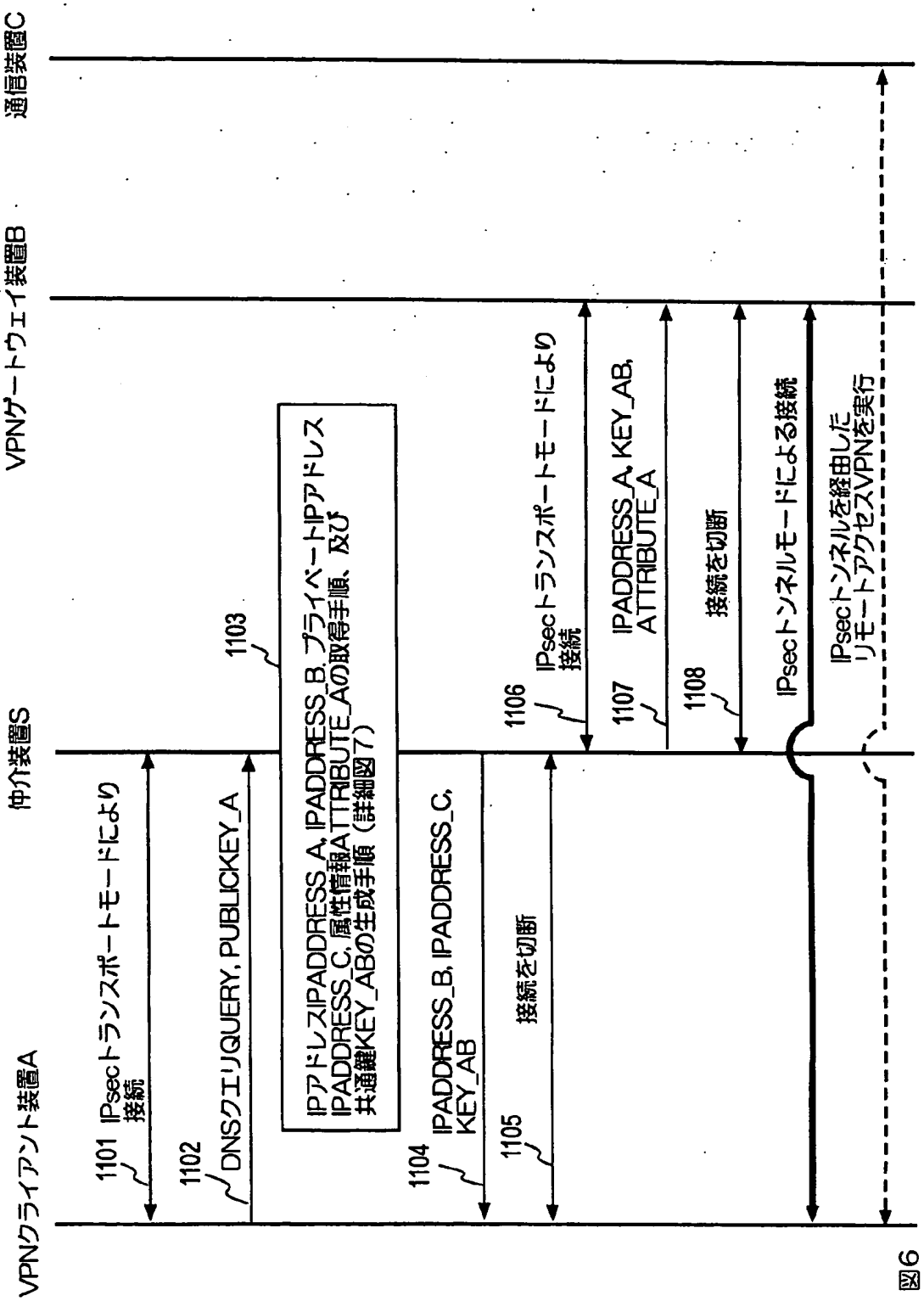

VPNクライアント装置A
仲介装置S
VPNゲートウェイ装置B
通信装置C
1101 IPsecトランスポートモードにより接続
1102 DNSクエリ QUERY, PUBLICKEY_A
1103
IPアドレスIPADDRESS_A, IPADDRESS_B, プライベートIPアドレスIPADDRESS_C, 属性情報ATTRIBUTE_Aの取得手順、及び共通鍵KEY_ABの生成手順（詳細図7）
1104 IPADDRESS_B, IPADDRESS_C, KEY_AB
1105 接続を切断
1106 IPsecトランスポートモードにより接続
1107 IPADDRESS_A, KEY_AB, ATTRIBUTE_A
1108 接続を切断
IPsecトンネルモードによる接続
IPsecトンネルを経由したリモートアクセスVPNを実行

図6

[図7]

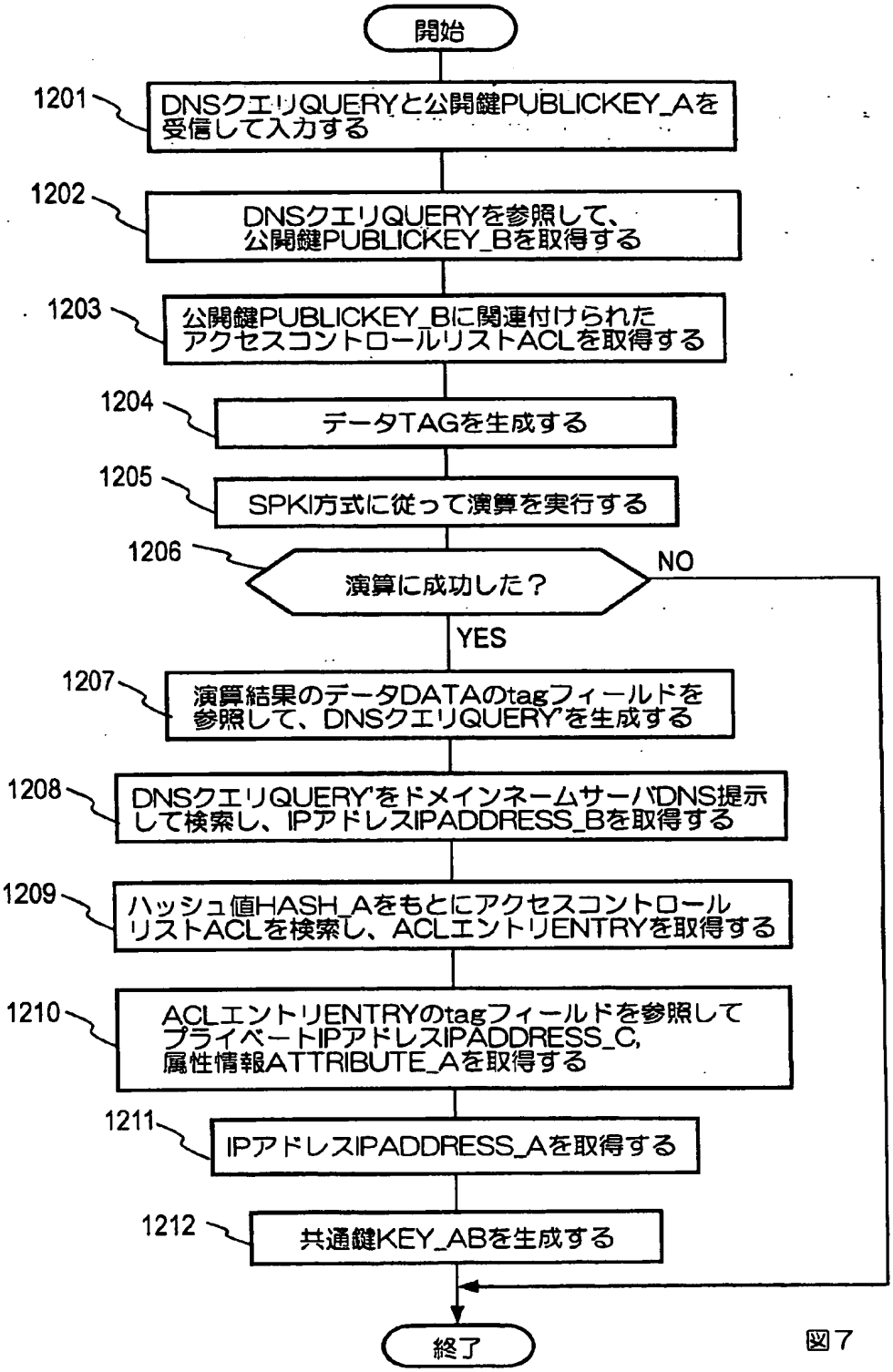

開始
1201
DNSクエリQUERYと公開鍵PUBLICKEY_Aを受信して入力する
1202
DNSクエリQUERYを参照して、公開鍵PUBLICKEY_Bを取得する
1203
公開鍵PUBLICKEY_Bに関連付けられたアクセスコントロールリストACLを取得する
1204
データTAGを生成する
1205
SPKI方式に従って演算を実行する
1206
演算に成功した？
NO
YES
1207
演算結果のデータDATAのtagフィールドを参照して、DNSクエリQUERY'を生成する
1208
DNSクエリQUERY'をドメインネームサーバDNS提示して検索し、IPアドレスIPADDRESS_Bを取得する
1209
ハッシュ値HASH_AをもとにアクセスコントロールリストACLを検索し、ACLエントリENTRYを取得する
1210
ACLエントリENTRYのtagフィールドを参照してプライベートIPアドレスIPADDRESS_C,属性情報ATTRIBUTE_Aを取得する
1211
IPアドレスIPADDRESS_Aを取得する
1212
共通鍵KEY_ABを生成する
終了

図7

[図8]

図８

```
(acl
  (entry
    (subject hash sha 1  |HASH_A|)
    (tag(dns ドメインネームサーバDNSの名前 (hash sha 1  |HASH_B|))
      (ip IPADDRESS_C)
      (attribute ATTRIBUTE_A))
    (propagate)
    (validity(not-before時刻データ )(not-after時刻データ ))
  )
)
```

[図9]

図９

```
(tag(dns ドメインネームサーバDNSの名前 (hash sha 1  |HASH_B|)))
```

データTAGとして定義されるデータ

[図10]

```
(cert
  (issuer Seif)
  (subject (hash sha 1  |HASH_A|))
  (tag(dns ドメインネームサーバDNSの名前 (hash sha 1  |HASH_B|)))
  (propagate)
  (validity(not-before時刻データ )(not-after時刻データ ))
)
```

演算結果データTAGとして定義されるデータ

図１０

[図11]

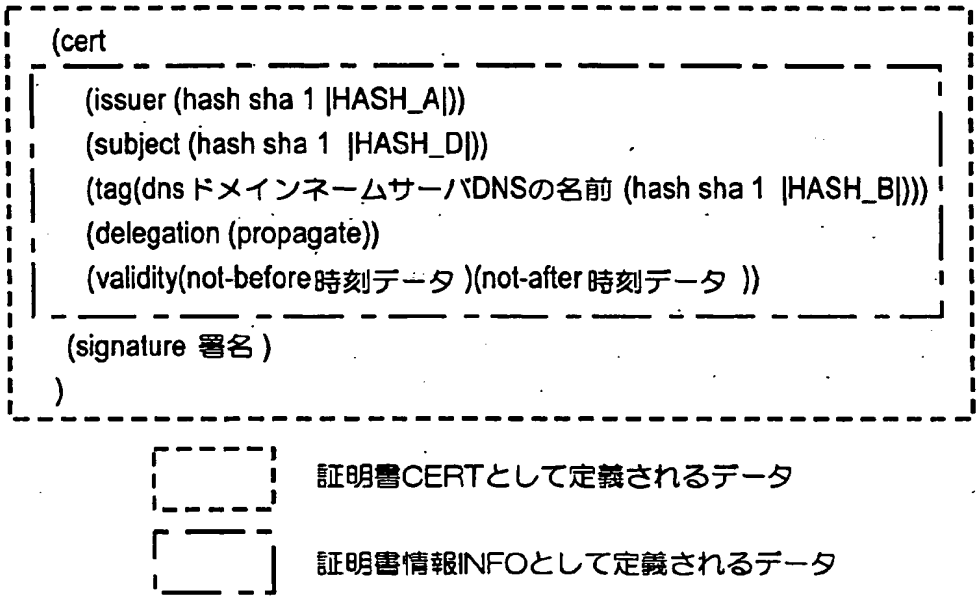

(cert
(issuer (hash sha 1 |HASH_A|))
(subject (hash sha 1 |HASH_D|))
(tag(dns ドメインネームサーバDNSの名前 (hash sha 1 |HASH_B|)))
(delegation (propagate))
(validity(not-before時刻データ)(not-after時刻データ))
(signature 署名)
)
証明書CERTとして定義されるデータ
証明書情報INFOとして定義されるデータ

図１１

[図12]

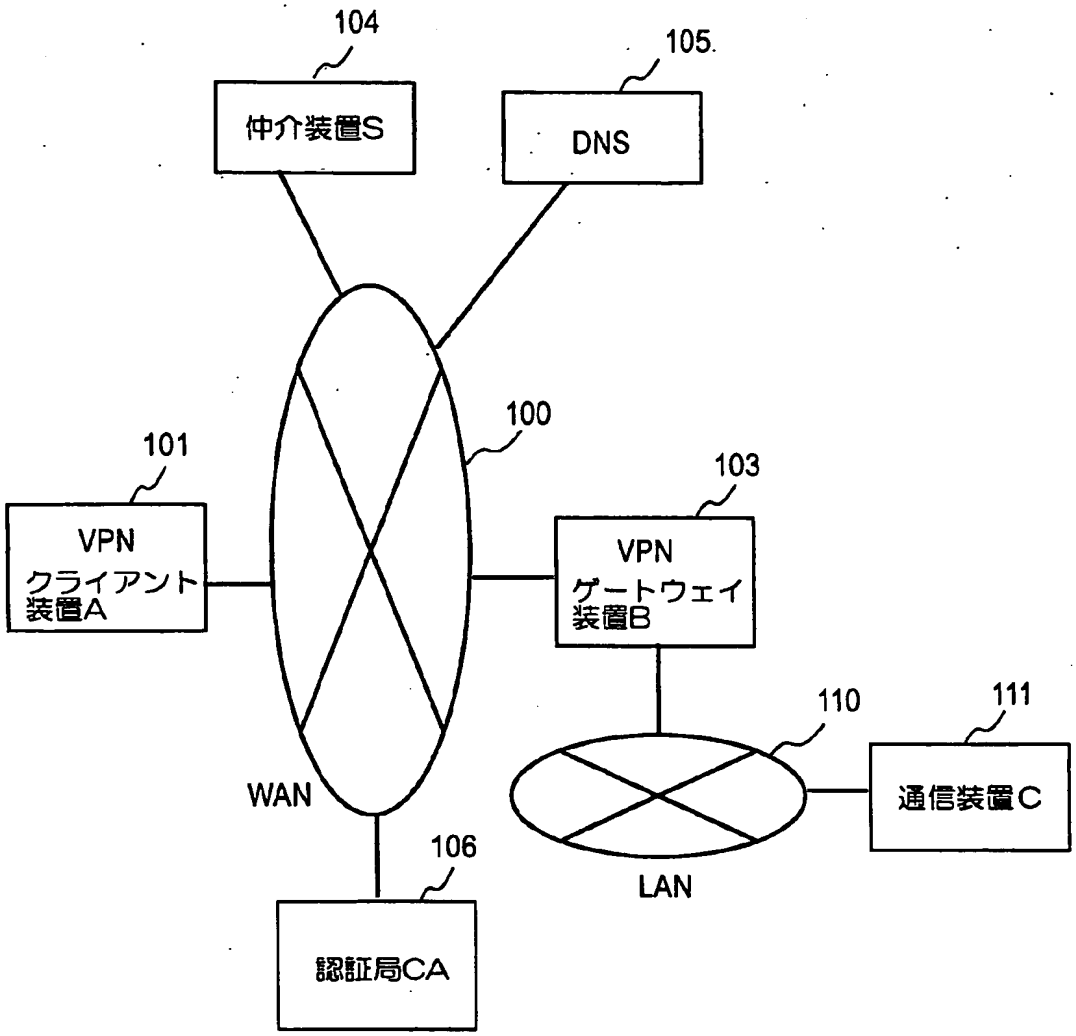

104
仲介装置S
105
DNS
100
101
VPN
クライアント
装置A
103
VPN
ゲートウェイ
装置B
110
111
通信装置C
WAN
LAN
106
認証局CA

図１２

[図13]

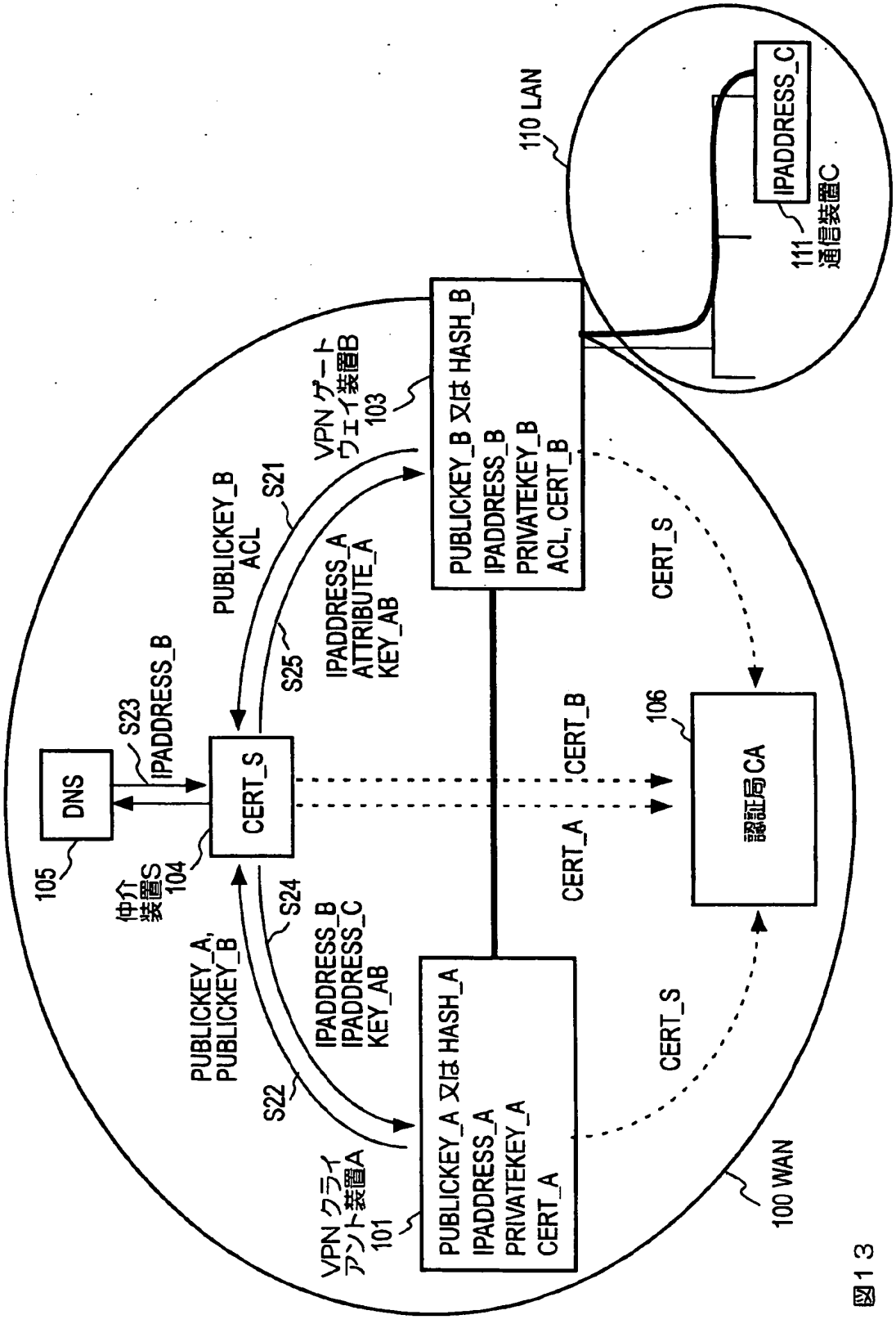

100 WAN
110 LAN
111 通信装置C
IPADDRESS_C
VPN クライアント装置A 101
VPN ゲートウェイ装置B 103
伸介装置S 104
105 DNS
106 認証局 CA
CERT_S
PUBLICKEY_A 又は HASH_A
IPADDRESS_A
PRIVATEKEY_A
CERT_A
PUBLICKEY_B 又は HASH_B
IPADDRESS_B
PRIVATEKEY_B
ACL, CERT_B
CERT_B
CERT_A
CERT_S
CERT_S
S21
PUBLICKEY_B
ACL
S22
PUBLICKEY_A,
PUBLICKEY_B
S23
IPADDRESS_B
S24
IPADDRESS_B
IPADDRESS_C
KEY_AB
S25
IPADDRESS_A
ATTRIBUTE_A
KEY_AB

図13

[図14]

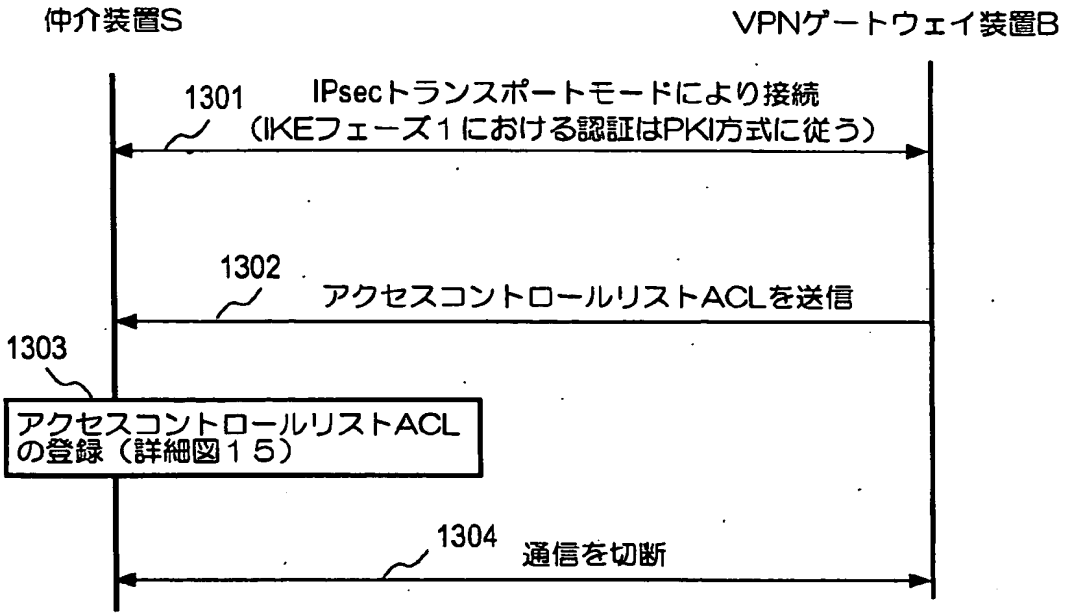


図１４

[図15]

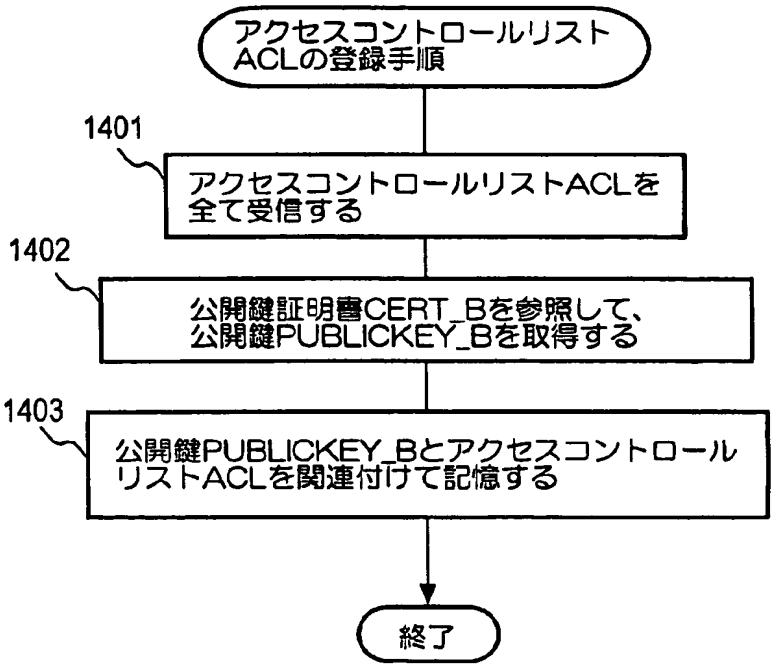


図１５

[図16]

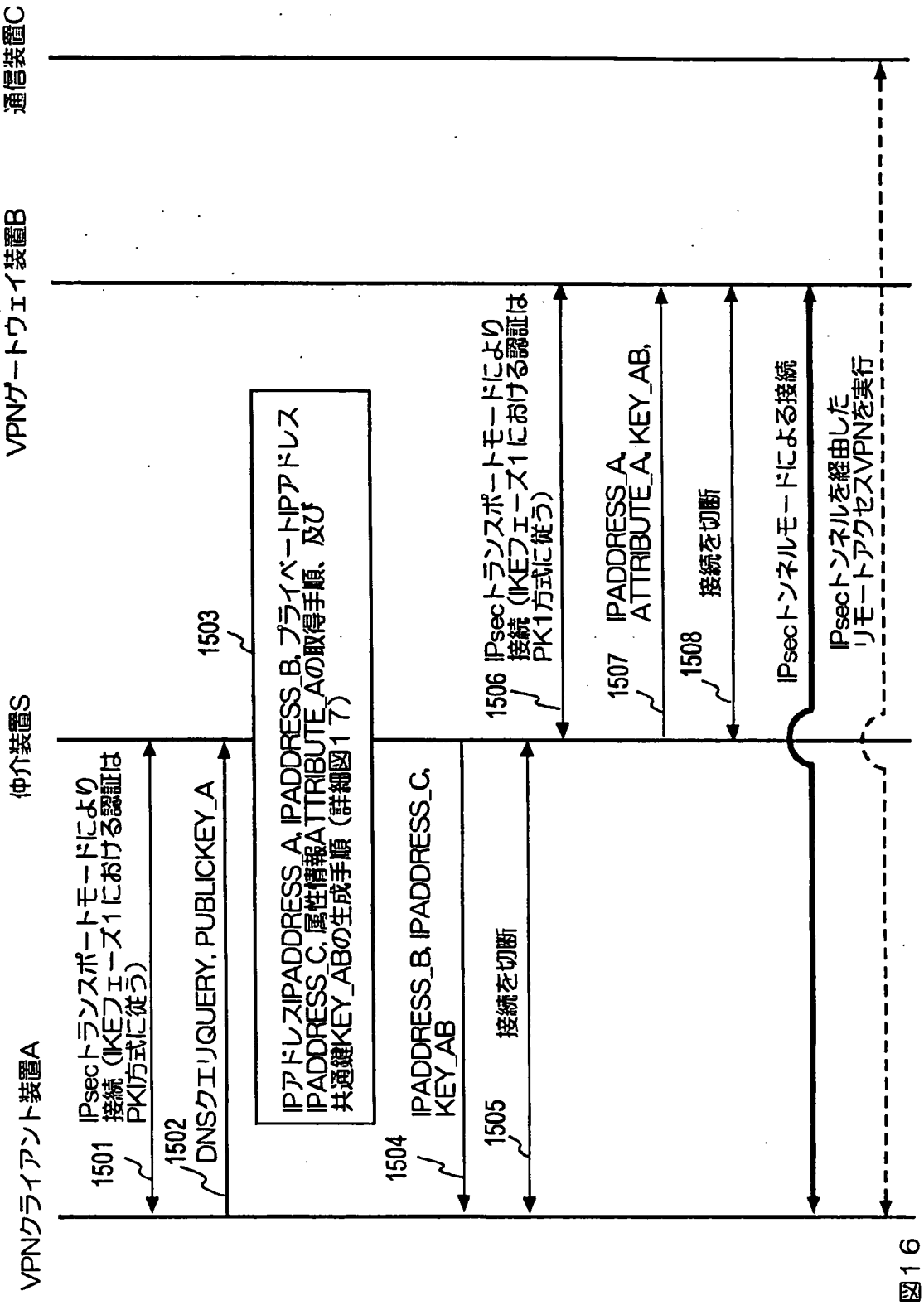

VPNクライアント装置A
仲介装置S
VPNゲートウェイ装置B
通信装置C
1501 IPsecトランスポートモードにより接続（IKEフェーズ1における認証はPKI方式に従う）
1502 DNSクエリQUERY, PUBLICKEY_A
1503 IPアドレスIPADDRESS_A, IPADDRESS_B, プライベートIPアドレスIPADDRESS_C, 属性情報ATTRIBUTE_Aの取得手順、及び共通鍵KEY_ABの生成手順（詳細図17）
1504 IPADDRESS_B, IPADDRESS_C, KEY_AB
1505 接続を切断
1506 IPsecトランスポートモードにより接続（IKEフェーズ1における認証はPK1方式に従う）
1507 IPADDRESS_A, ATTRIBUTE_A, KEY_AB,
1508 接続を切断
IPsecトンネルモードによる接続
IPsecトンネルを経由したリモートアクセスVPNを実行

図16

[図17]

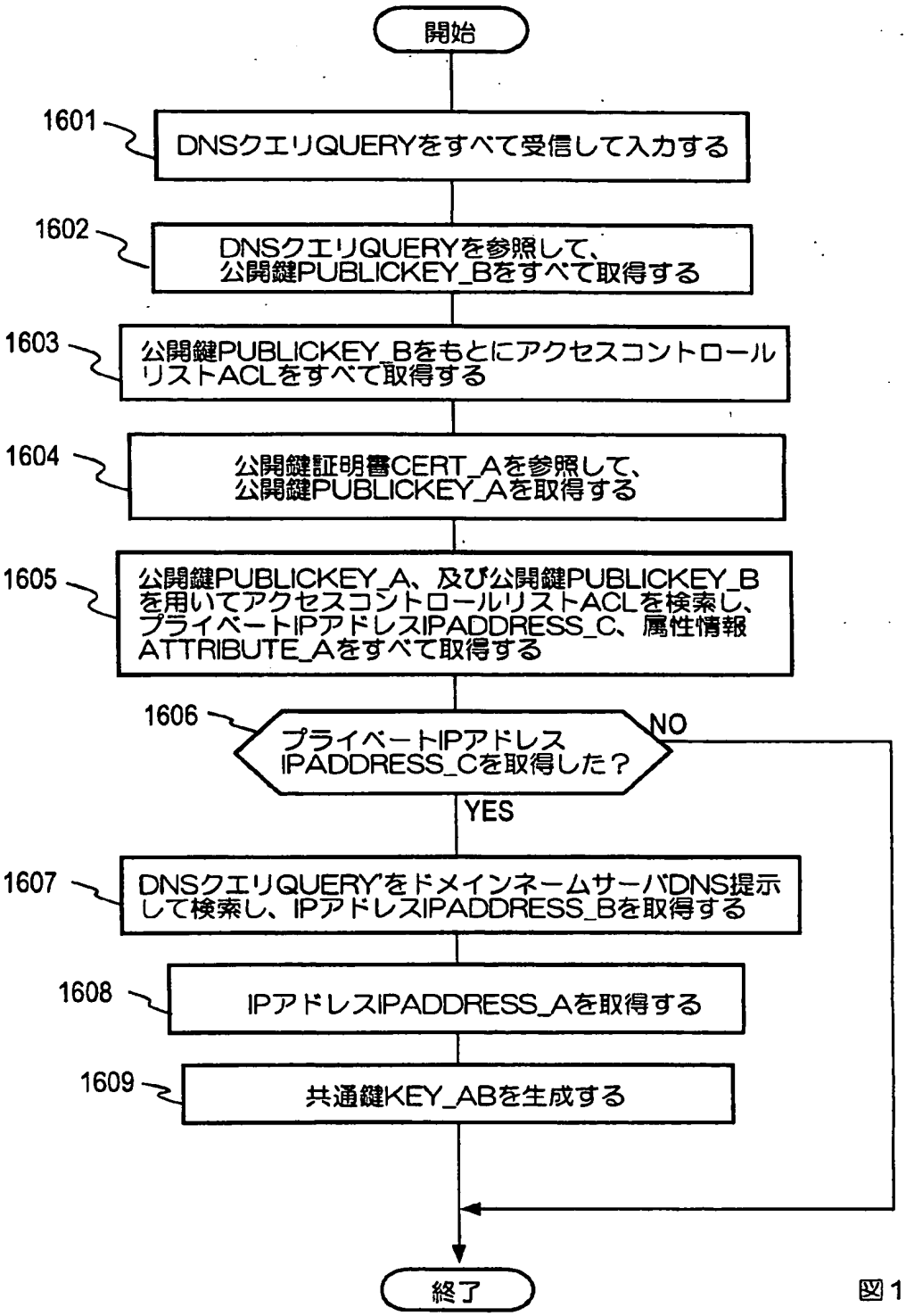

開始
1601
DNSクエリQUERYをすべて受信して入力する
1602
DNSクエリQUERYを参照して、
公開鍵PUBLICKEY_Bをすべて取得する
1603
公開鍵PUBLICKEY_Bをもとにアクセスコントロール
リストACLをすべて取得する
1604
公開鍵証明書CERT_Aを参照して、
公開鍵PUBLICKEY_Aを取得する
1605
公開鍵PUBLICKEY_A、及び公開鍵PUBLICKEY_B
を用いてアクセスコントロールリストACLを検索し、
プライベートIPアドレスIPADDRESS_C、属性情報
ATTRIBUTE_Aをすべて取得する
1606
プライベートIPアドレス
IPADDRESS_Cを取得した？
NO
YES
1607
DNSクエリQUERY'をドメインネームサーバDNS提示
して検索し、IPアドレスIPADDRESS_Bを取得する
1608
IPアドレスIPADDRESS_Aを取得する
1609
共通鍵KEY_ABを生成する
終了

図１７

[図18]

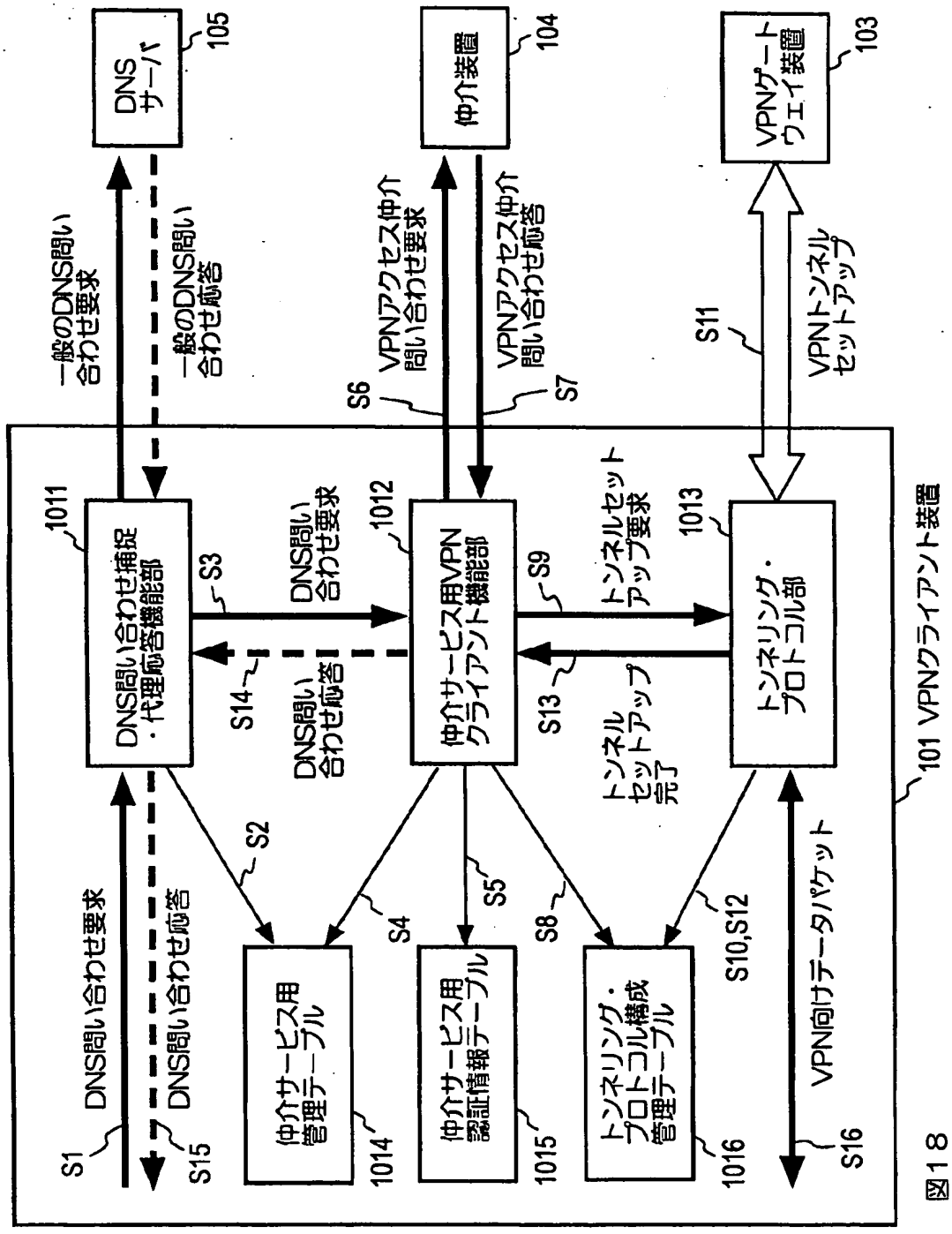

DNS サーバ
105
仲介装置
104
VPNゲートウェイ装置
103
一般のDNS問い合わせ要求
一般のDNS問い合わせ応答
VPNアクセス仲介問い合わせ要求
VPNアクセス仲介問い合わせ応答
VPNトンネルセットアップ
S6
S7
S11
1011
DNS問い合わせ捕捉・代理応答機能部
S3
DNS問い合わせ要求
1012
仲介サービス用VPNクライアント機能部
S9
トンネルセットアップ要求
1013
トンネリング・プロトコル部
S14
DNS問い合わせ応答
S13
トンネルセットアップ完了
S1
DNS問い合わせ要求
S15
DNS問い合わせ応答
S2
S4
S5
S8
S10,S12
S16
VPN向けデータパケット
仲介サービス用管理テーブル
1014
仲介サーバ用認証情報テーブル
1015
トンネリング・プロトコル構成管理テーブル
1016
101 VPNクライアント装置

図18

[図19]

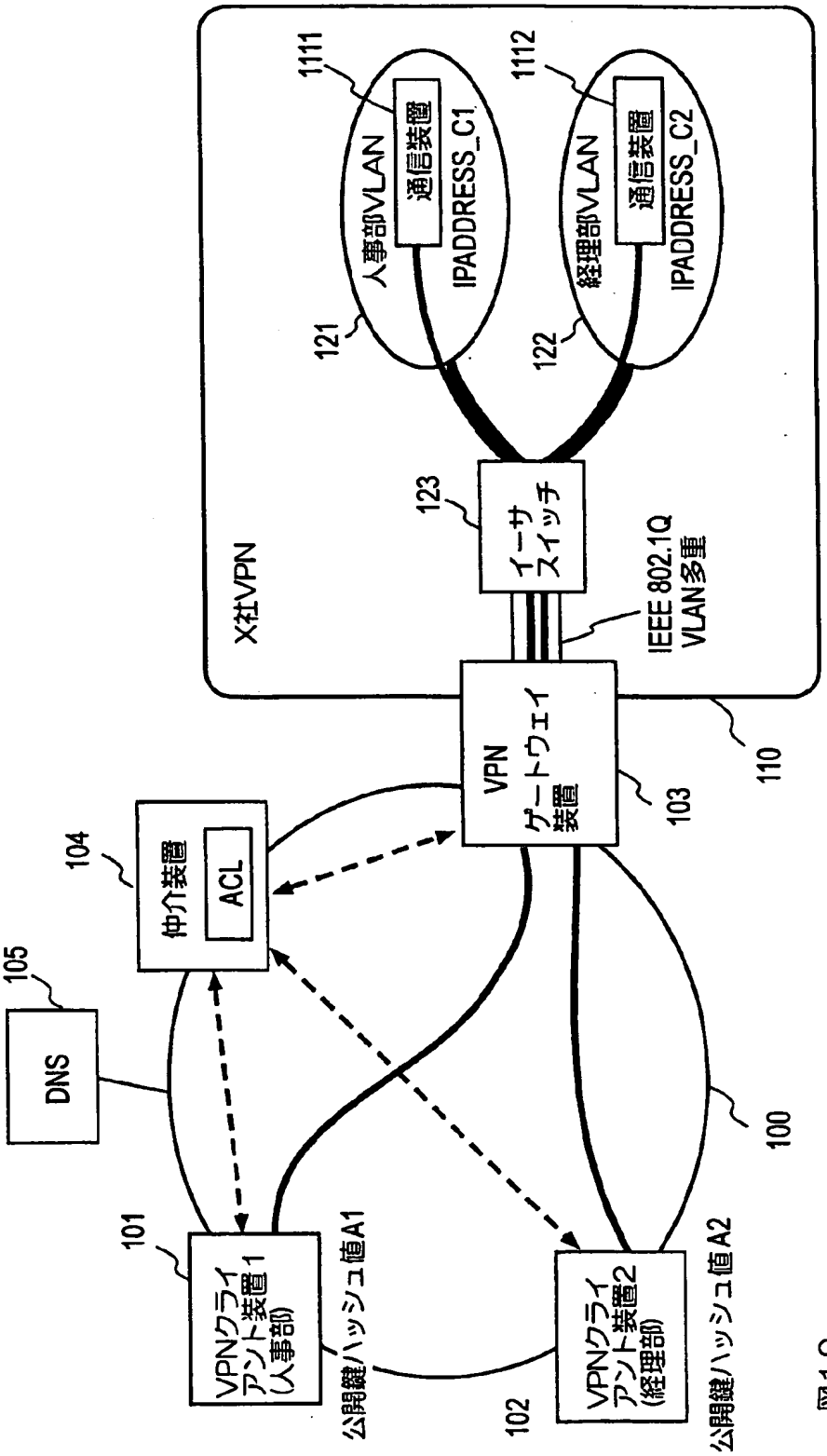

X社VPN
1111
人事部VLAN
通信装置
IPADDRESS_C1
121
1112
経理部VLAN
通信装置
IPADDRESS_C2
122
123
イーサスイッチ
IEEE 802.1Q
VLAN多重
VPN
ゲートウェイ
装置
103
110
104
仲介装置
ACL
105
DNS
100
101
VPNクライアント装置1
(人事部)
公開鍵ハッシュ値A1
102
VPNクライアント装置2
(経理部)
公開鍵ハッシュ値A2

図19

[図20]

```
(acl                                    VPNクライアント装置A1のためのエントリ
 (entry
    (subject hash sha1  |HASH_A1|)
    (tag(dns ドメインネームサーバDNSの名前 (hash sha1  |HASH_B|))
       (ip IPADDRESS_C1)
       (attribute(VLAN 人事部 VLAN)))
    (propagate)
    (validity(not-before時刻データ )(not-after 時刻データ ))
 )
                                        VPNクライアント装置A2のためのエントリ
 (entry
    (subject hash sha1  |HASH_A2|)
    (tag(dns ドメインネームサーバDNSの名前 (hash sha1  |HASH_B|))
       (ip IPADDRESS_C2)
       (attribute(VLAN 経理部 VLAN)))
    (propagate)
    (validity(not-before時刻データ )(not-after 時刻データ ))
 )
)
```

図２０

[図21]

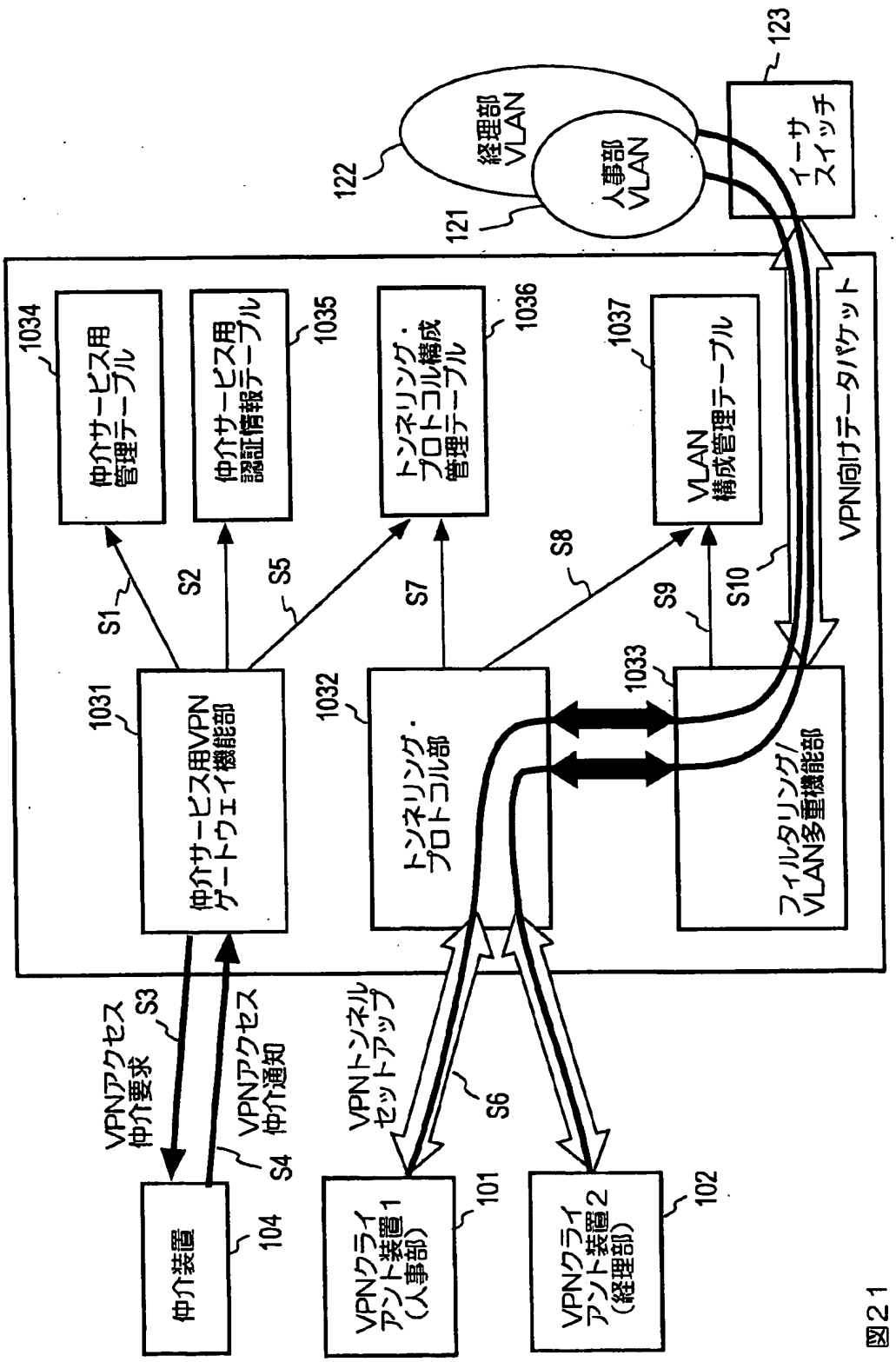

123
イーサスイッチ
122
経理部VLAN
人事部VLAN
121
VPN向けデータパケット
1034
仲介サービス用管理テーブル
1035
仲介サービス用認証情報テーブル
1036
トンネリング・プロトコル構成管理テーブル
1037
VLAN構成管理テーブル
S1
S2
S5
S7
S8
S9
S10
1031
仲介サービス用VPNゲートウェイ機能部
1032
トンネリング・プロトコル部
1033
フィルタリング/VLAN多重機能部
VPNアクセス仲介要求
S3
VPNアクセス仲介通知
S4
VPNトンネルセットアップ
S6
104
仲介装置
101
VPNクライアント装置1(人事部)
102
VPNクライアント装置2(経理部)

図21

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009446

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho (Y1,Y2) 1926-1996 Toroku Jitsuyo Shinan Koho (U) 1994-2004
Kokai Jitsuyo Shinan Koho (U) 1971-2004 Jitsuyo Shinan Toroku Koho (Y2) 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 3009876 B2 (Nippon Telegraph And Telephone Corp.), 14 February, 2000 (14.02.00), Fig. 27 & JP 11-177582 A & US 6307837 B1	1-15
A	JP 3454788 B2 (Nippon Telegraph And Telephone Corp.), 06 October, 2003 (06.10.03), Fig. 4 & JP 2002-185538 A	1-15

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 September, 2004 (28.09.04)	19 October, 2004 (19.10.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009446

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-208965 A (NEC Corp., NTT Communications Kabushiki Kaisha), 26 July, 2002 (26.07.02), Abstract (Family: none)	1-15

国際調査報告

国際出願番号 PCT／JP2004／009446

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl⁷ H04L 12／56

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl⁷ H04L 12／56

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報（Y1，Y2）	1926－1996年
日本国公開実用新案公報（U）	1971－2004年
日本国登録実用新案公報（U）	1994－2004年
日本国実用新案登録公報（Y2）	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 3009876 B2（日本電信電話株式会社），2000.02.14，図27 & JP 11-177582 A & US 6307837 B1	1－15
A	JP 3454788 B2（日本電信電話株式会社），2003.10.06，図4 & JP 2002-185538 A	1－15

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 28.09.2004	国際調査報告の発送日 19.10.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 小林紀和　5X　4240 電話番号 03－3581－1101 内線 3556

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００２－２０８９６５　Ａ（日本電気株式会社、エヌ・ティ・ティ・コミュニケーションズ株式会社），２００２．０７．２６，【要約】（ファミリなし）	１－１５